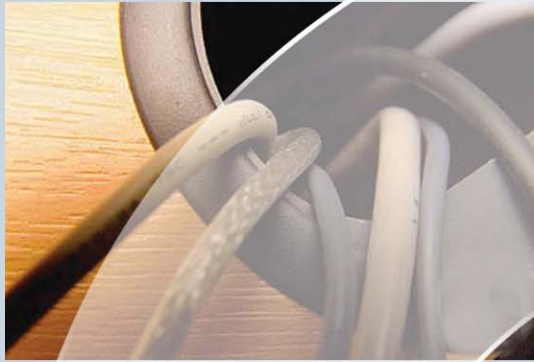


F R O S T



S U L L I V A N



SÉCURITÉ E-MAIL  
« À LA DEMANDE » :  
PEUT-ELLE VRAIMENT  
TENIR SES PROMESSES ?



## **TABLE OF CONTENTS**

Introduction .....	3
Fonctionnement des services de sécurité e-mail « à la demande » .....	4
Réponse aux préoccupations liées à sécurité e-mail « à la demande » .....	7
Analyse du Coût Total de Possession des options de sécurité e-mail .....	8
Avantages des services de sécurité e-mail « à la demande » .....	12
BlackSpider Technologies .....	14
Conclusion .....	17

## INTRODUCTION

Au cours des premières années d'existence du marché des services gérés, les objections concernant les avantages de l'offre de services étaient élevées. Ces services étaient perçus comme étant inutilisables et consommateurs de temps en raison d'une accumulation des coûts et des niveaux de complexité. Le terme " à la demande " est en train de se substituer au terme " service géré ", et les sociétés comme Salesforce.com et IBM modifient la perception des entreprises concernant la manière dont les achats, la gestion et la livraison des logiciels et des services peuvent être effectués. Le succès du marché de la sécurité a donné naissance en particulier à une vague de remises en question chez les administrateurs de réseaux, la plupart se mettant en relation avec des pairs satisfaits des services fournis par leur fournisseur de sécurité " à la demande ". Étant donné les avantages que représente cette approche ainsi que la réputation et les compétences toujours en progrès des fournisseurs de services, de plus en plus d'entreprises envisagent à présent le recours à des alternatives externalisées en matière de sécurité.

La messagerie électronique est une application vitale pour les entreprises. De nos jours, les compagnies s'appuient sur le courrier électronique pour la productivité et la continuité opérationnelle au même titre que tout autre processus central. Cependant, sur le plan de la sécurité, l'e-mail est à l'origine de sérieuses inquiétudes puisque la plupart des employés ont accès à des messages électroniques pouvant être utilisés pour véhiculer toutes sortes de données, y compris des programmes malveillants.

La sécurisation des messages électroniques peut représenter une tâche fastidieuse pour les entreprises. C'est à ce niveau que les fournisseurs de services de sécurité e-mail " à la demande " spécialisés peuvent jouer un rôle essentiel pour protéger efficacement les systèmes de communication par e-mail d'une compagnie.

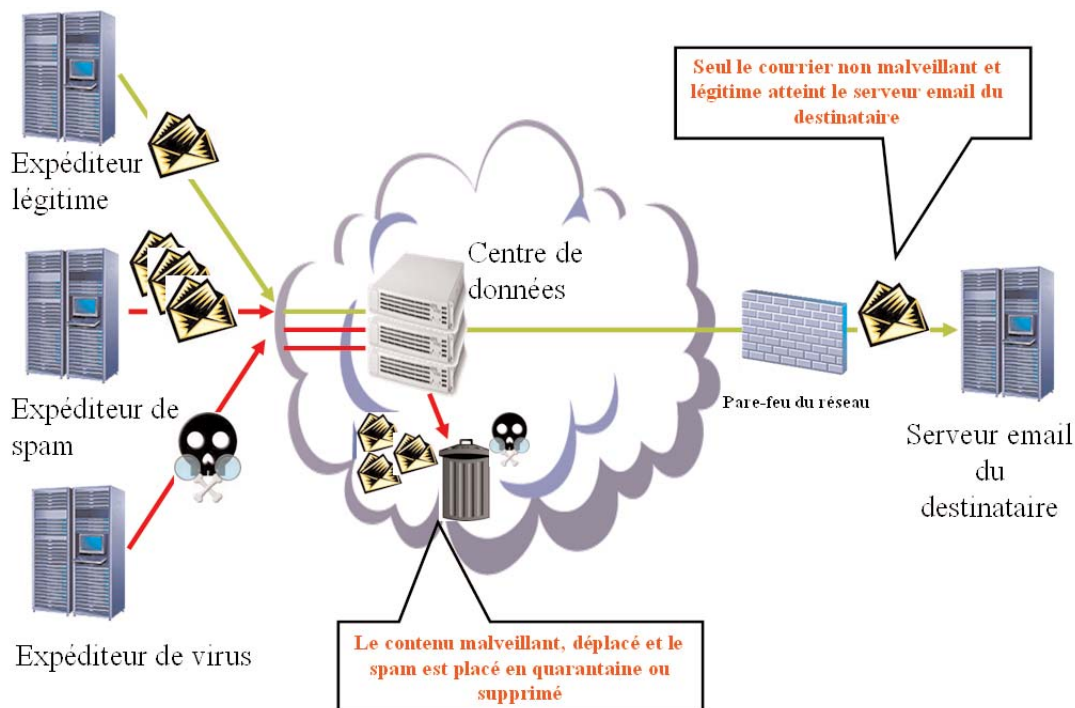
## Fonctionnement des services de sécurité e-mail " à la demande "

Le schéma n°1 illustre le processus des services de sécurité e-mail " à la demande ". Le fournisseur de services intercepte l'e-mail adressé sur le domaine de l'utilisateur et filtre ce message avant qu'il puisse atteindre le serveur de messagerie du destinataire. Ceci constitue un bon moyen d'empêcher les pièces jointes malveillantes, les spywares (" espionciels "), les usurpations d'identité (ou " phishing "), le spam et tout autre courrier indésirable de pénétrer sur le réseau de l'entreprise, et évite ainsi toute attaque malveillante.

Les meilleurs fournisseurs de services sont capables de scanner des dizaines de millions de courriers électroniques provenant de l'extérieur des réseaux de l'entreprise, et ce 7 jours sur 7 et 24 heures sur 24. Grâce à des équipes composées d'experts entièrement dédiés à la sécurité informatique, ces fournisseurs permettent d'accroître le niveau de protection vis-à-vis des menaces connues et inconnues et de réduire le niveau de trafic Internet indésirable, comme le spam et les virus, pouvant obstruer l'infrastructure d'une entreprise.

La plupart des fournisseurs de services permettent aux utilisateurs de configurer les options de filtrage pour empêcher les faux positifs. Tout comme pour les logiciels de filtrage sur site, les administrateurs ont l'autorisation d'établir des listes noires et/ou des listes blanches afin de garantir que les courriers indésirables n'atteignent pas le système de l'entreprise et pour ne pas bloquer le courrier légitime tentant d'accéder à son serveur de messagerie.

### Schéma n°1 : Processus des services de sécurité e-mail " à la demande "



Source : Frost & Sullivan

## Types d'options de sécurité e-mail

Puisque les e-mails représentent des risques accrus pour la sécurité et une augmentation des coûts pour les administrateurs, de nombreuses solutions ont émergé pour combattre ces menaces et ces nuisances. Les solutions de sécurité e-mail varient en terme de capacités et de stratégie d'intégration, mais se répartissent en deux grandes catégories : les solutions basées sur les produits et les solutions basées sur les services.

### Solutions basées sur les produits

#### *Solutions basées sur les appareils*

Les appareils de sécurité e-mail sont du matériel " hardware " dédié, équipé préalablement d'applications logicielles et de systèmes d'exploitation permettant de fournir à l'utilisateur une solution prête à l'emploi. Ces appareils sont déployés au niveau de la passerelle de la compagnie et se comportent en " gardiens " chargés d'empêcher le courrier indésirable de pénétrer dans le réseau.

#### *Solutions basées sur les logiciels*

Les solutions logicielles peuvent s'acheter indépendamment du matériel existant. Dans le cadre de cette option d'installation, le client fournit le serveur sur lequel le logiciel est exécuté. Ce serveur peut être un nouveau serveur, dédié ou hautement performant, ou bien un serveur de messagerie existant dans le réseau de l'entreprise.

#### *Solutions basées sur les services*

Les solutions basées sur les services ne sont pas mises en place dans le réseau de l'entreprise. À la place, tout le trafic e-mail destiné au réseau du client est acheminé par l'intermédiaire de l'équipement du fournisseur de services afin de scanner et de filtrer ce courrier. Ensuite, le trafic e-mail scanné est soit réacheminé vers le client pour remise du courrier, soit bloqué conformément à la politique de sécurité du client.

Pour déterminer leur stratégie de sécurité, les entreprises doivent décider entre une solution basée sur les produits ou sur les services, en choisissant la formule la mieux adaptée à ses exigences. Cette décision doit se baser sur plusieurs paramètres dont :

- Le coût total de la solution ;
- Le niveau de protection ;
- L'efficacité de la solution ; et
- Les ressources disponibles en interne.

Le schéma n°2 met en évidence les principaux avantages et inconvénients des produits et services dédiés à la sécurité des communications e-mail, et propose une conclusion.

**Schéma n°2 : Avantages et inconvénients des solutions de sécurité e-mail basées sur les produits ou sur les services**

	<b>Solution basée sur les produits</b>	<b>Solution basée sur les services</b>	<b>Conclusion</b>
<b>Pour</b>	<ul style="list-style-type: none"> <li>▪ Flexibilité de personnalisation pour l'utilisateur final</li> <li>▪ Nombre relativement bas de faux positifs</li> <li>▪ Baisse du trafic bloqué au niveau de la passerelle</li> <li>▪ Contrôle total envers la solution et le processus de gestion du courrier électronique</li> </ul>	<ul style="list-style-type: none"> <li>▪ Meilleure protection : Multiconstructeur</li> <li>▪ Soutien assuré par une équipe d'experts travaillant 24h/24 et 7j/7</li> <li>▪ Mise en place rapide"</li> <li>▪ Sécurité accrue : <ul style="list-style-type: none"> <li>♦ Dissimulation des utilisateurs e-mail</li> <li>♦ Élimination des attaques DOS</li> </ul> </li> <li>▪ Faible nombre de faux positifs</li> <li>▪ CTP généralement plus faible : <ul style="list-style-type: none"> <li>♦ Réduction des coûts d'exploitation</li> <li>♦ Réduction des coûts de bande passante</li> <li>♦ Économies de personnel</li> <li>♦ Libération des ressources informatiques</li> </ul> </li> </ul>	<p><b>Il est fortement recommandé à toute compagnie d'utiliser un service de sécurité " à la demande " pour ses communications e-mail, à condition d'avoir trouvé un fournisseur de services digne de confiance et répondant à ses besoins, sauf dans le cas où le niveau d'expertise, la qualité de service et/ou les économies sur les coûts opérationnels sont supérieurs en interne</b></p>
<b>Contre</b>	<ul style="list-style-type: none"> <li>▪ CTP généralement plus élevé : <ul style="list-style-type: none"> <li>♦ Coûts de gestion et d'administration élevés</li> <li>♦ Surcharge de la bande passante et du stockage, surtout pour les solutions avec serveurs</li> <li>♦ Défi pour l'entreprise en matière d'évolutivité</li> </ul> </li> <li>▪ Difficulté de recrutement de personnel spécialisé</li> </ul>	<ul style="list-style-type: none"> <li>▪ Sentiment de perte de contrôle</li> <li>▪ Le niveau de personnalisation proposé par certains fournisseurs n'est pas satisfaisant</li> <li>▪ Temps de latence pour envoyer et recevoir des e-mails, même si dans la plupart des cas ceci est imperceptible</li> <li>▪ Certains fournisseurs ont des difficultés au niveau de l'évolutivité</li> </ul>	

Source : Frost & Sullivan

## **Réponse aux préoccupations liées à sécurité e-mail " à la demande "**

Le schéma n°2 illustre certaines des préoccupations principales associées avec les solutions de sécurité basées sur les services. Nous sommes convaincus que ces inquiétudes sont issues à la fois de conceptions erronées et de questions historiques, mais les fournisseurs de services d'aujourd'hui ont déployé beaucoup d'efforts pour dissiper ces préoccupations. Nous nous sommes donc penchés individuellement sur la validité de chacune de ces préoccupations.

### ***Sentiment de perte de contrôle***

Chez certaines personnes, il existe une conception erronée selon laquelle les administrateurs informatiques perdent le contrôle de leurs réseaux lorsqu'ils utilisent des services de sécurité " à la demande ". Les administrateurs sont tout particulièrement préoccupés par le risque de perdre leur capacité de contrôle et de réaction en temps réel face aux problèmes qui touchent la sécurité de leur réseau lorsqu'ils utilisent une solution basée sur les services. En réalité, les fournisseurs de services de sécurité e-mail permettent souvent aux administrateurs informatiques d'avoir un contrôle total de la solution, en leur accordant un accès complet et la possibilité d'effectuer en temps réel les modifications nécessaires sur les paramètres de leur politique de sécurité.

### ***Faible niveau de personnalisation***

Une autre conception erronée consiste à dire que les services de sécurité " à la demande " ne permettent pas aux administrateurs informatiques d'avoir la flexibilité nécessaire pour personnaliser leurs paramètres de sécurité dans le but de répondre à leurs exigences particulières. La nature de cette crainte est de penser qu'en utilisant un service de sécurité " à la demande ", les administrateurs informatiques seront soumis à une politique de sécurité de type " taille unique ". Les fournisseurs de services gérés peuvent en fait proposer un niveau de personnalisation très élevé, permettant aux administrateurs de définir des politiques de sécurité pour différents groupes d'utilisateurs voire d'individus. Par exemple, les paramètres privés du PDG d'une entreprise pourront être différents de ceux attribués à ses employés.

### ***Temps de latence des communications***

Un autre sujet de préoccupation soulevé par les administrateurs informatiques est le temps de latence généré par le routage de leurs e-mails par l'intermédiaire d'un fournisseur de services " à la demande ". En raison de la dépendance envers des systèmes échappant à leur contrôle, certains administrateurs sont inquiets et se demandent si les e-mails de grande importance pourront être envoyés et reçus à temps. En réalité, la plupart des fournisseurs de services de communication peuvent traiter les e-mails en quelques secondes sans perturber l'utilisation habituelle des communications par e-mail. De plus, la réduction de la charge de travail concernant les e-mails (plus de la moitié des e-mails étant généralement supprimés ou mis en quarantaine) a des effets positifs sur la performance du serveur de messagerie de l'entreprise.

### ***Problèmes d'évolutivité***

Les administrateurs informatiques font souvent part de leurs inquiétudes quant aux capacités des fournisseurs de services en matière d'évolutivité lors de l'ajout d'un nouveau service ou de la migration d'un client vers un environnement plus grand. Ceci pouvait être le cas dans le passé mais de nos jours les meilleurs fournisseurs de services de sécurité e-mail " à la demande " disposent de centres opérationnels de sécurité de haut niveau. Ces centres leur donnent la possibilité de répondre aux besoins de toutes les entreprises, quelle que soit leur taille.

## **Analyse du Coût Total de Possession des options de sécurité e-mail**

Les administrateurs effectuent souvent une analyse initiale concernant le retour sur investissement (ROI " Return on Investment ") des produits, en comparant le coût du produit ou du service face au coût ou au risque que présente la menace. Afin de mesurer avec précision le différentiel de coûts, les administrateurs ont besoin d'une méthode d'évaluation leur permettant de comprendre non seulement le coût du système en tant que tel, mais aussi l'utilisation et la maintenance de ce système. Le Coût Total de Possession (CTP) correspond à la quantification des coûts associés à l'installation, à la configuration, à la gestion et à la maintenance d'un système en plus du coût d'achat initial du système. Les paragraphes suivants étudient les coûts parfois cachés, associés à l'installation d'une solution de sécurité e-mail .

### **Planification**

La planification nécessite l'examen des politiques de sécurité actuelles de l'entreprise, afin de comprendre comment la solution s'intégrera à la politique de sécurité actuelle et comment elle la modifiera. À ce stade une liste des produits et des services requis, dont l'achat est prévu, doit être établie. Il convient de noter, entre autres éléments supplémentaires de planification, quand et comment la solution sera livrée dans les différents bureaux, comment les administrateurs intégreront la solution, et comment seront réparties les responsabilités concernant ces tâches.

Les coûts liés à la phase de planification sont basés principalement sur les coûts du personnel participant à ce processus et/ou la participation de consultants externes. Plus une solution est complexe, plus le coût de planification est important.

### **Prix d'achat**

Le prix d'achat de la solution de sécurité e-mail correspond au coût d'achat du produit ou du service et peut inclure le prix d'un appareil (dans le cas de l'achat d'un produit) ou d'un service, ainsi que les frais de licence correspondants. Les frais de licence pour les solutions basées sur les services sont assez simples à calculer, mais ils ne sont pas facilement quantifiables pour les solutions basées sur les logiciels / le matériel " hardware " ; ceci s'explique par le fait que cela ne comprend pas uniquement la licence d'utilisation de la solution, mais également les coûts de prolongation des garanties, de support technique, et des autres éléments accompagnant le produit ou service de sécurité e-mail.

Afin de garantir l'ininterruption de l'activité de l'entreprise, toute solution de sécurité doit intégrer une fonctionnalité de redondance. Pour les solutions basées sur les produits, la compagnie doit se charger elle-même de mettre en place cette fonctionnalité, par exemple en faisant l'acquisition de systèmes de sauvegarde. Pour les solutions basées sur les services, les fournisseurs de services intègrent généralement cette fonctionnalité de redondance comme partie intégrante de leur offre. Lorsqu'une solution est composée de produits provenant de fabricants multiples, les dispositions en matière de licences d'utilisation peuvent devenir plus complexes car les fabricants ont généralement des approches différentes les uns des autres en matière de licences.

Pour les produits de sécurité e-mail basés sur les appareils, le coût de la plateforme " hardware " est compris dans le prix d'achat. Néanmoins, de nombreuses solutions sont proposées aujourd'hui sous forme de solutions logicielles uniquement, ce qui signifie que l'approvisionnement et l'installation d'une plateforme séparée pour le matériel " hardware " sur lequel le logiciel sera exécuté seront peut-être nécessaires. Dans ce cas, des coûts de planification supplémentaires pourront alors être encourus car les administrateurs devront décider du niveau de performance acceptable et des exigences de débit ; ceci peut compliquer le processus décisionnel quant au choix du matériel " hardware " à acheter. Les solutions basées sur les services ont l'avantage de fournir à l'entreprise un processus d'achat simplifié puisque les frais annuels comprennent les coûts de licence et de support technique.

*! Cette analyse ne comprend pas les avantages indirects, comme les économies de bande passante réalisées, et qu'il conviendra de comptabiliser lors du calcul exhaustif du CTP.*

## **Approvisionnement**

Les coûts d'approvisionnement peuvent varier en fonction des habitudes d'approvisionnement et des procédures mises en place par la compagnie. Les coûts d'approvisionnement sont liés au temps passé à contacter un vendeur, qu'il s'agisse d'un revendeur ou d'un fournisseur vendant ses solutions directement, à négocier un prix d'achat, et à effectuer la commande. Si une solution n'est pas disponible immédiatement, un temps d'attente supplémentaire sera peut-être nécessaire avant que la solution soit livrée chez l'acheteur. Ces coûts comprennent également le temps nécessaire pour le processus de validation de l'achat. Les dépenses d'approvisionnement peuvent se creuser si la solution de sécurité e-mail est mise en place dans des bureaux situés sur différents sites géographiques. En règle générale, ces coûts sont minimes et s'appliquent à la fois à l'achat de solutions basées sur les produits et à celles basées sur les services. Toutefois, pour les solutions basées sur les logiciels uniquement, les coûts d'approvisionnement peuvent être plus élevés car plusieurs fournisseurs ou revendeurs peuvent intervenir dans l'achat de la plateforme " hardware ".

## **Installation de la plateforme**

Des coûts supplémentaires interviennent lors de l'installation des logiciels sur les plateformes " hardware ". La complexité de ce processus augmente généralement avec la nécessité de transformer le dispositif en passant d'un serveur multifonctionnel à un composant d'infrastructure sécurisé et renforcé. Ce processus de renforcement de la sécurité implique le retrait de tous les services qui ne sont pas nécessaires à l'exécution de tâches limitées et spécifiques affectées au dispositif de filtrage du courrier. L'exclusion de ces services supplémentaires assure une protection contre les vulnérabilités et l'exploitation de ces services inutiles. Même s'il existe de nombreux documents de référence relatifs aux meilleures pratiques à suivre pour renforcer la sécurité des serveurs, cette tâche peut être complexe pour les administrateurs de sécurité informatique non qualifiés (cette tâche est également consommatrice de temps même pour les professionnels les plus qualifiés). Normalement, ces coûts n'interviennent pas pour les solutions basées sur les services puisqu'il n'est généralement pas nécessaire d'installer du matériel ou des logiciels supplémentaires.

## **Intégration**

Les coûts d'intégration peuvent s'appliquer à la fois aux solutions basées sur les produits et à celles basées sur les services, et concernent l'installation physique d'un dispositif dans l'infrastructure du réseau, ou la configuration d'un service nécessaire au réseau. Cette intégration peut nécessiter la modification des paramètres, le réacheminement du flux de trafic (réglage de l'agent de transfert de messages " Message Transfer Agent (MTA) " et de l'enregistrement d'échange de courrier " Mail Exchange Record (MX) "), et la modification des composants d'infrastructure, afin de permettre au système de fonctionner correctement. Souvent, de nombreux services informatiques de petite taille font appel aux services d'un consultant pour être conseillés quant aux procédures à suivre pour effectuer ces modifications correctement et empêcher ainsi tout risque de mauvaise configuration pouvant occasionner une défaillance du système. Généralement, les solutions basées sur les produits génèrent un coût d'intégration plus élevé que les solutions basées sur les services pour lesquelles les processus d'intégration peuvent se traduire simplement par une modification des enregistrements d'échange de courrier.

## **Configuration**

Les tâches de configuration concernent les réglages devant être effectués après l'installation initiale de la solution dans le réseau. Après la mise en place de la solution, de nombreuses configurations doivent être effectuées concernant la sensibilité des filtres et les types de spam devant être bloqués. Des décisions supplémentaires en matière de configuration doivent être prises pour le traitement du courrier suspect, à savoir le bloquer, le mettre en quarantaine, le supprimer ou le stocker.

Des paramètres de stockage doivent être définis afin de déterminer la durée pendant laquelle le spam sera stocké ainsi que la taille maximum de l'espace de stockage disponible devant être alloué. En tenant compte de la nécessité d'effectuer ces configurations pour chaque utilisateur, cette tâche peut rapidement devenir complexe et consommatrice de temps puisque les divers utilisateurs souhaiteront mettre en place des politiques de sécurité différentes pour éviter les faux positifs et les faux négatifs. Les solutions basées sur les produits et celles basées sur les services génèrent toutes les deux des coûts de configuration dans une certaine mesure. Toutefois, dans le cas des solutions basées sur les services, le processus de configuration peut être simplifié considérablement, puisque les politiques de sécurité peuvent souvent être configurées par l'intermédiaire d'un portail en ligne.

## **Contrôles**

Après l'accomplissement des tâches d'installation et de configuration, les administrateurs doivent continuellement surveiller la solution pour s'assurer de sa précision et de son efficacité. Des contrôles de performance garantissant un débit et un niveau de retard acceptables sont effectués pour vérifier que la solution fonctionne de manière optimale. Ceci consiste à surveiller l'infrastructure du réseau et les politiques de sécurité, et ce, pendant toute la durée de vie de la solution. Lorsque les conditions sont inférieures aux conditions idéales, des réglages de configuration sont également effectués lors de cette phase.

Les coûts de contrôle comprennent les coûts correspondant au personnel chargé de surveiller la solution et aux applications utilisées à cet effet. Les solutions basées sur les produits et celles basées sur les services génèrent toutes les deux des coûts de contrôle mais dans le cas des solutions basées sur les services, ces coûts se limitent au contrôle de la politique de sécurité. Souvent, les entreprises utilisent de multiples produits de sécurité afin de se protéger contre les menaces immédiates dites du " jour zéro ". Ceci rend non seulement les réseaux plus complexes mais accroît également les coûts de contrôle correspondants. Les fournisseurs de services " à la demande " disposent d'une technologie heuristique privée et d'équipes de recherche Internet surveillant les menaces Internet, ce qui leur permet de réagir automatiquement face aux menaces immédiates.

## **Mises à niveau**

Même si les mises à niveau sont parfois proposées gratuitement, les mises à niveau des produits les plus importants, intervenant environ tous les ans, sont généralement facturées par le fournisseur/revendeur. L'investissement continu dans l'amélioration des produits doit être pris en compte et les exigences budgétaires doivent être définies pour permettre l'acquisition de ces mises à niveau. Ces mises à niveau apportent généralement des améliorations considérables aux solutions basées sur les produits, mais elles peuvent également générer des difficultés en matière d'interopérabilité et de configuration lors de leur mise en place. De plus, l'achat et l'installation de ces mises à niveau renvoient l'utilisateur au premier facteur CTP et nécessitent que l'acheteur exécute l'ensemble du processus à nouveau. Grâce au modèle du fournisseur de services, le fournisseur se charge de ces changements, ce qui s'effectue généralement en douceur pour le client.

## **Correctifs pour les logiciels**

Comme ne le savent que trop bien les administrateurs de réseaux des services informatiques d'aujourd'hui, l'utilisation de correctifs est devenue une solution régulière face aux vulnérabilités en constante évolution, identifiées sur les réseaux de sécurité. À la complexité des besoins en matière de correctifs, s'ajoute la nécessité d'identifier les correctifs suffisamment importants pour être mis en place, et la tâche de plus en plus importante consistant à tester les correctifs avant leur mise en place dans l'environnement en réseau. En l'absence de ces tests, les correctifs s'exposent aux mêmes inconvénients que les mises à niveau : des problèmes éventuels d'interopérabilité ou de configuration. À nouveau, grâce au modèle du fournisseur de services, les tâches relatives aux correctifs sont prises en charge par le fournisseur de services, ce qui est une préoccupation de moins pour les administrateurs.

## Fin de vie

Dans le cas des solutions basées sur les produits, qu'il s'agisse du logiciel de sécurité e-mail ou du matériel " hardware ", ou les deux, ces solutions devront un jour ou l'autre être remplacées. Les mises à niveau des principaux logiciels peuvent nécessiter une réinstallation complète de la solution et les capacités du matériel en matière de performance devront tôt ou tard être mises à jour à l'aide de nouvelles plateformes. Lorsqu'il est nécessaire de remplacer l'un des composants de base de la solution e-mail ou les deux, l'ensemble de la liste CTP doit être réexaminée.

Dans le modèle du fournisseur de services, l'entreprise n'a pas besoin de se préoccuper de ces considérations puisque le fournisseur de services se charge généralement de la responsabilité consistant à gérer la transition de ses systèmes. Comme pour les mises à niveau, ces transitions sont généralement conçues pour occasionner un minimum de perturbations sur le service fourni. Lorsqu'un service " à la demande " arrive en fin de contrat, la compagnie devra effectuer une analyse CTP pour l'aider à :

- Déterminer si ses besoins sont toujours satisfaits au mieux par un service " à la demande " ; et
- Le cas échéant, évaluer les offres disponibles auprès de différents fournisseurs.

Le schéma n°3 présente un comparatif des facteurs CTP que les compagnies doivent prendre en compte pour choisir une solution basée sur les produits ou sur les services, pour leur sécurité e-mail.

### Schéma n°3 : Facteurs CTP des solutions de sécurité e-mail basées sur les produits ou sur les services

Facteur CTP	Activités/Détails	Solution basée sur les produits	Solution basée sur les services
Planification	<ul style="list-style-type: none"> <li>■ Examen des options/caractéristiques disponibles</li> <li>■ Analyse CTP</li> <li>■ Délégation des responsabilités</li> <li>■ Modification de la politique de sécurité</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>
Achats	<ul style="list-style-type: none"> <li>■ Serveur</li> <li>■ Licences des logiciels</li> <li>■ Appareil</li> <li>■ Mises à niveau des signatures/règles</li> <li>■ Assurance de remplacement</li> <li>■ Licence annuelle par utilisateur</li> <li>■ Frais d'activation</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>X</li> </ul>	<ul style="list-style-type: none"> <li>X</li> <li>X</li> <li>X</li> <li>X</li> <li>X</li> <li>✓</li> <li>✓</li> </ul>
Approvisionnement	<ul style="list-style-type: none"> <li>■ Contrat distributeur/fournisseur</li> <li>■ Négociation des prix</li> <li>■ Processus de validation des achats</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> </ul>
Installation de la plateforme	<ul style="list-style-type: none"> <li>■ Renforcement de la sécurité du serveur</li> <li>■ Installation des logiciels</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>X</li> <li>X</li> </ul>
Intégration	<ul style="list-style-type: none"> <li>■ Modification des infrastructures</li> <li>■ Intégration des appareils</li> <li>■ Configuration MTA/MX</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>X</li> <li>X</li> <li>✓</li> </ul>
Configuration	<ul style="list-style-type: none"> <li>■ Configuration initiale des caractéristiques</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> </ul>
Contrôles	<ul style="list-style-type: none"> <li>■ Contrôle des performances/activités</li> <li>■ Réglages de configuration récurrents</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>
Mises à niveau	<ul style="list-style-type: none"> <li>■ Planification, achat et approvisionnement des mises à niveau</li> <li>■ Intégration des mises à niveau</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>X</li> <li>X</li> </ul>
Correctifs	<ul style="list-style-type: none"> <li>■ Intégration semestrielle des correctifs</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>X</li> </ul>
Fin de vie	<ul style="list-style-type: none"> <li>■ Modification des infrastructures</li> <li>■ Démontage des appareils</li> <li>■ Configuration MTA/MX</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> </ul>	<ul style="list-style-type: none"> <li>X</li> <li>X</li> <li>✓</li> </ul>

Source : Frost & Sullivan

## **Avantages des services de sécurité e-mail " à la demande "**

Nous sommes convaincus que, en fonction des capacités et des besoins d'une entreprise, les services de sécurité e-mail " à la demande " peuvent présenter des avantages considérables. Laisser un fournisseur de services fiable et digne de confiance se charger de la sécurité et de la protection des communications par e-mail peut constituer une approche bien plus fiable et économique pour beaucoup d'entreprises que de se charger elles-mêmes de ces tâches. Nous avons examiné en détail chacun des avantages clés suivants.

### **Économies sur les coûts opérationnels**

Les administrateurs n'ont pas besoin de passer énormément de temps sur les questions de sécurité e-mail, y compris la gestion du système, sa configuration et l'application de correctifs. Nos services évitent l'encombrement de la bande passante du réseau par du courrier indésirable et la diminution de la taille de l'espace de stockage du serveur de messagerie à cause de ces messages indésirables. Par ailleurs, les utilisateurs ne perdent pas de temps à supprimer le courrier indésirable. Enfin, le temps d'indisponibilité suite à l'infiltration d'un virus sur le réseau par e-mail est réduit.

### **Réduction du CTP**

Le coût d'un service de sécurité " à la demande " est généralement inférieur au coût généré par l'emploi à plein temps d'une équipe d'experts en sécurité travaillant en interne, et par l'investissement dans des solutions basées sur des logiciels et/ou du matériel " hardware ". Un fournisseur de services peut répartir sur plusieurs clients les investissements réalisés dans le matériel " hardware ", les logiciels, les installations, et les analystes, et donc réduire le coût par client.

### **Absence de la contrainte de recrutement d'un spécialiste**

Le manque de personnel informatique qualifié spécialisé dans la sécurité génère une pression sur les services informatiques, contraints de recruter du personnel spécialisé, de le former, de le rémunérer et de le retenir. Le coût d'emploi de ces spécialistes de la sécurité informatique peut être très élevé et de nombreuses entreprises n'ont pas les moyens financiers de recruter de tels professionnels. En utilisant des solutions basées sur les services, les coûts d'embauche, de formation, et de rétention de personnel hautement qualifié deviennent la responsabilité du fournisseur de services.

### **Équipe d'experts en sécurité " à la demande "**

Un membre du personnel travaillant en interne et chargé de la sécurité informatique uniquement à temps partiel ou qui ne constate qu'un nombre limité d'incidents liés à la sécurité n'est probablement pas aussi expérimenté qu'une personne qui effectue le même travail à plein temps, constate l'impact de la sécurité sur plusieurs clients différents, et qui développe des solutions de sécurité dotées de possibilités d'application plus larges. En étant confrontés quotidiennement à des situations de menaces informatiques potentielles, les fournisseurs de services disposent d'une connaissance des questions de sécurité reposant sur une solide expérience.

### **Aide à la mise en conformité avec les réglementations**

Il existe plusieurs initiatives d'ordre réglementaire contraignant les entreprises des différents secteurs d'activité à accroître leurs niveaux de sécurité. Les réglementations généralement citées sont les suivantes:

- Loi " Health Insurance Portability Accountability Act (HIPAA) " sur la transférabilité et la responsabilité des assurances médicales ;
- Loi Gramm-Leach-Bliley Act (GLB) ;  
Sécurité intérieure (" Homeland Security ") ;
- Loi Sarbanes-Oxley ; et
- Loi européenne " European Data Protection Act " sur la protection des données.

Les différentes directives relatives à la protection des données dans des pays comme le Royaume-Uni et l'Allemagne, et d'autres mandats en matière de sécurité, ont créé pour de nombreuses entreprises une pression vis-à-vis de la réglementation et une augmentation des budgets. Les capacités d'audit et de reporting inhérentes aux rapports sur le Web des fournisseurs de services e-mail " à la demande " entraînent, chez de nombreux clients, l'utilisation des informations ainsi trouvées pour répondre aux exigences de la législation et des équipes d'audit. Les clients sont généralement convaincus que le fait d'externaliser le contrôle et la maintenance de leur équipement auprès de professionnels de la sécurité répond à l'obligation mal définie de " due diligence " (prudence nécessaire) mise en avant par ces législations.

Pour l'utilisateur final, susceptible de se demander s'il doit gérer les questions de sécurité en interne ou non, la charge supplémentaire que représente la mise en conformité avec les réglementations et, dans une plus grande mesure, les pénalités sanctionnant un niveau de sécurité inférieur à la moyenne, accroît la valeur reconnue de l'idée d'utiliser un service de sécurité. Les fournisseurs de services de sécurité e-mail " à la demande " peuvent aider à conserver des enregistrements de tous les e-mails et de tous les fichiers accédés par qui que ce soit. Ces enregistrements sont conservés aussi longtemps que les données sous-jacentes sont disponibles dans le système.

Comme les services e-mail " à la demande " offrent des avantages potentiels importants pour les entreprises, il est donc nécessaire de bien comprendre en détail la nature de l'offre disponible auprès des fournisseurs de services. Dans cette optique, nous avons travaillé avec BlackSpider Technologies, un fournisseur de services européen spécialisé dans la sécurité e-mail et Web " à la demande ", afin de bien comprendre leur approche et la nature de leur offre.

## **BlackSpider Technologies**

Basée au Royaume-Uni, BlackSpider Technologies est également solidement implantée en France et en Allemagne. Depuis sa création en 2002, BlackSpider Technologies est devenue la société de services de sécurité "à la demande" dont la croissance est la plus rapide à l'échelle européenne. BlackSpider dispose d'une équipe d'intervention dédiée aux situations d'urgence qui se concentre sur l'identification des nouvelles menaces et le développement de protections contre ces menaces. Sa technologie propriétaire permet d'identifier et de bloquer les menaces immédiates dès qu'elles surviennent. En février 2006, la société est parvenue à bloquer 60.000 copies d'un nouveau virus plus de 50 heures avant la diffusion de la première signature de ce virus. L'offre de services BlackSpider comprend la conception, l'achat (produits et support), la mise en place et l'intégration de la solution, ainsi que la gestion opérationnelle. Ceci permet aux clients de l'entreprise de se concentrer sur la gestion de l'application.

### **Les services**

BlackSpider propose deux offres de service principales : MailControl, son service de sécurité e-mail, et WebDefence, son service de filtrage Web dont l'action est complémentaire à celle de ses services e-mail existants.

### **MailControl**

MailControl fournit une protection totale contre les virus transmis par courrier, le spam et les contenus déplacés, ainsi qu'un cryptage du courrier électronique pour assurer la sécurité des communications e-mail. MailControl est suite intégrée de services modulaires entièrement "à la demande" (anti-virus, anti-spam, filtrage des contenus et cryptage). Elle fournit une sécurité e-mail totale sans nécessiter de matériel ou de logiciels supplémentaires, et associe les technologies de pointe des meilleurs fabricants de solutions dédiées à la sécurité des contenus. Les services de MailControl sont basés sur la technologie de prévision intelligente Huntsman de BlackSpider, ce qui permet l'analyse des menaces e-mail et la réactualisation des modes de défense en temps réel, simplifiant ainsi la définition et l'application de la politique de sécurité de l'entreprise. Tout le courrier est acheminé par l'intermédiaire du réseau de distribution mondial de grande fiabilité de BlackSpider, grâce à des centres de données dédiés situés dans toute l'Europe et aux États-Unis. Par ailleurs, MailControl fournit des fonctions en libre-service à la disposition des utilisateurs et des outils de gestion des quarantaines, ainsi que des statistiques à la demande et des rapports sur les messages.

## **WebDefence**

WebDefence est une suite intégrée de services "à la demande" garantissant une protection totale face aux menaces Web, comme les virus, les spyware ("espionciels"), les usurpations d'identité (ou attaques de type "hameçonnage", de l'anglais phishing), les vers, les chevaux de Troie et autres programmes malveillants. WebDefence permet également de contrôler l'accès Web des employés. Tout comme MailControl, WebDefence utilise également la technologie de prévention Huntsman qui permet de fournir en temps réel des informations sur les menaces Web et une protection contre ces menaces. WebDefence donne également à ses utilisateurs la possibilité d'effectuer des modifications des politiques en temps réel.

### **Les facteurs de différenciation**

En comparaison avec des solutions de gestion alternatives menées en interne, BlackSpider fournit manifestement de plus hauts niveaux de protection permettant aux clients de garder le contrôle total de leurs politiques de sécurité tout en réalisant des économies considérables. BlackSpider fournit à ses clients:

- La garantie d'un service continu grâce à son réseau mondial ;
- Une évolutivité sans limites ; et
- Un choix de modules basés sur les besoins du client.

Son approche de protection multiniveau offre une garantie supplémentaire à ses clients puisque ce système ne peut pas être testé par les auteurs des virus et a donc permis de bloquer toutes les attaques virales depuis son lancement.

L'un des principaux clients de BlackSpider est la branche européenne d'un fabricant mondial d'électronique pour le grand public (que nous appellerons "l'Entreprise"), auquel BlackSpider fournit des services de sécurité e-mail "à la demande". L'étude de cas suivante met en évidence les problèmes auxquels l'Entreprise devait faire face au niveau de sa sécurité e-mail, et décrit le processus engagé ayant conduit au choix de BlackSpider comme fournisseur de services de sécurité e-mail "à la demande" de cette Entreprise.

## Étude de cas : Fabricant mondial d'électronique pour le grand public

### **L'Entreprise**

L'Entreprise est en activité en Europe depuis le début des années 1960, date à laquelle elle établit son premier bureau commercial en Allemagne. L'Entreprise a étendu sa présence dans toute l'Europe suite à un important investissement dans les activités commerciales et de fabrication.

### **Le problème**

L'Entreprise reconnut avoir un problème de sécurité e-mail. Elle menait en interne ses activités de scan des e-mails, de gestion, et de définition des politiques, et ceci était devenu un processus de plus en plus fastidieux et coûteux. Elle estima donc qu'il était nécessaire de se pencher sur d'autres possibilités, y compris l'intervention d'un tiers digne de confiance chargé de gérer l'ensemble du processus de sécurité à sa place. Ce fut une étape importante pour l'Entreprise car il s'agissait là de la première fois qu'elle envisageait d'externaliser son système e-mail, même en partie.

### **Le processus**

En mars 2005, l'Entreprise rechercha sur le marché un fournisseur de services ayant fait ses preuves, offrant une qualité de services supérieure, et pouvant lui accorder le même niveau de contrôle que si sa sécurité e-mail était gérée en interne.

BlackSpider figura parmi les finalistes, aux côtés d'un autre fournisseur de services spécialisé, en fonction de critères techniques et de références. Les deux solutions furent testées en interne de manière approfondie, au cours d'un processus qui dura plusieurs mois.

### **Les résultats**

BlackSpider fut choisie en janvier 2006 pour assurer la protection de l'ensemble des 6.500 utilisateurs e-mail ; cette décision fut motivée par les facteurs suivants :

- BlackSpider offrait une meilleure protection contre les attaques virales grâce à l'utilisation de moteurs de scan provenant de trois différents fournisseurs, en association avec sa propre technologie ;
- BlackSpider offrait la meilleure solution anti-spam pour l'Entreprise en raison de ses options, sa granularité et son aisance de configuration ;
- BlackSpider permettait à l'Entreprise de conserver le même niveau de contrôle envers les utilisateurs et les politiques, y compris la mise en place de différentes politiques pour divers groupes d'utilisateurs ;
- BlackSpider proposait une aide et des services de support au Royaume-Uni et en Allemagne, c'est-à-dire dans les pays où les activités de l'Entreprise étaient les plus importantes en Europe ;
- La performance de service de BlackSpider lors des différents tests, conduisit l'Entreprise à penser qu'aucun courrier électronique important pour l'Entreprise ne se retrouverait bloqué ; et enfin
- La raison la plus importante fut la réactivité de BlackSpider et l'ouverture de son approche qui permirent de gagner le respect et la confiance d'une compagnie aussi exigeante que l'Entreprise.

## CONCLUSION

Les communications e-mail sont essentielles dans le monde professionnel d'aujourd'hui, mais de nombreuses entreprises sont dépassées par le spam, les risques de sécurité causés par les virus et les vers transmis par courrier électronique, les usurpations d'identité et les spyware, ainsi que les implications en matière de responsabilité en cas d'e-mails de nature pornographique ou renfermant tout autre contenu indésirable. Il est de plus en plus difficile pour les administrateurs de réseaux d'assurer le contrôle de toutes ces menaces.

L'une des solutions consiste à consacrer davantage de ressources, à augmenter les investissements dans les produits dédiés à la sécurité des contenus, et à tenter de gérer l'ensemble du processus en interne. Une autre solution consiste à faire appel à un fournisseur de services de sécurité e-mail " à la demande " spécialisé. Cette formule est de plus en plus populaire auprès des entreprises qui :

- Ne disposent pas du personnel dédié à ce processus,
- Ne souhaitent pas gérer leur sécurité en interne ; et/ou
- Cherchent à réduire leurs coûts.

Frost & Sullivan est convaincu que BlackSpider est dotée d'une approche et d'un profil d'expert lui offrant une position très favorable en tant que partenaire potentiel auprès des sociétés souhaitant adopter une solution de sécurité d'e-mail " à la demande ".

## "A PROPOS DE FROST & SULLIVAN

*Frost & Sullivan, une société de conseil en stratégies de croissance à portée globale fondée il y a plus de 40 ans, agit en collaboration avec ses clients pour créer de la valeur à travers des stratégies de croissance novatrices. Ce partenariat est fondé sur notre plateforme « Growth Partnership Services » par laquelle nous fournissons des études sur les industries, des stratégies de marketing, des conseils et de la formation à nos clients dans le but de les aider à développer leurs affaires. L'avantage essentiel que Frost & Sullivan apporte à ses clients est une perspective globale sur une vaste gamme d'industries, de marchés, et de technologies, et sur des données économétriques et démographiques. Avec une clientèle qui comprend des sociétés parmi les 1 000 premières à un niveau mondial, des entreprises émergentes ainsi que la communauté financière, Frost & Sullivan est devenue l'une des plus grandes sociétés de conseil spécialisées en problématiques de croissance dans le monde. Pour plus d'informations consultez: [www.frost.com](http://www.frost.com).*

### *Copyright*

*Tous droits réservés. Le contenu du document est strictement confidentiel et constitue la propriété exclusive de Frost & Sullivan. Aucune partie ne peut être distribuée, citée, copiée ou reproduite autrement sans consentement écrit explicite de Frost & Sullivan."*