

Hosted Email Security

Un service de sécurité Cloud mutualisé qui protège des menaces de messagerie évoluées actuelles.

Les e-mails sont le principal moyen de communication à l'échelle mondiale des entreprises de toutes tailles. Les e-mails sont aussi le premier vecteur de menace pour les cyberattaques. Les menaces de messagerie ont évolué. Les campagnes de spams de masse et d'e-mails de phishing ont été remplacées par des attaques de phishing particulièrement ciblées qui peuvent véhiculer des ransomware et logiciels malveillants de type zero-day. Elles peuvent aussi prendre la forme d'attaques BEC (Business Email Compromise) qui visent les virements bancaires ou les informations confidentielles. Les solutions antispam et anti-logiciels malveillants traditionnelles ne permettent pas de stopper cette nouvelle vague d'attaques de phishing évoluées. Qui plus est, d'après les réglementations gouvernementales, votre entreprise peut désormais avoir des comptes à rendre concernant la protection des données confidentielles, les mesures prises pour éviter les fuites et enfin la sécurisation des échanges d'e-mails contenant des informations sensibles ou personnelles de clients.

Pour se protéger de ces menaces en perpétuelle mutation, les entreprises doivent déployer une solution de sécurité multicouche qui va au-delà du simple antispam et anti-logiciels malveillants. Cette solution doit inclure des fonctionnalités de protection avancées et dédiées, et protéger contre les pièces jointes et URL malveillantes, ainsi que contre les attaques par imposteur. Par ailleurs, la gestion et la maintenance d'une solution de sécurisation de messagerie sur site peuvent s'avérer onéreuses et chronophages. Les organisations ont donc tout à gagner de remplacer leur solution héritée par une solution de sécurisation de messagerie hébergée abordable et facile à utiliser, qui s'intègre facilement à leur infrastructure de messagerie existante, qui peut être configurée rapidement et sans frais initiaux, et qui réagit dynamiquement

aux nouvelles menaces tout en réduisant les dépenses administratives régulières et la complexité.

SonicWall Hosted Email Security offre une protection supérieure basée sur le cloud contre les menaces entrantes et sortantes, y compris les ransomware, le phishing, le BEC (Business Email Compromise), le spoofing, les spams et les virus, pour un prix d'abonnement mensuel ou annuel abordable, prévisible et flexible. Parallèlement, ce service réduit en amont le temps et les coûts de déploiement ainsi que les dépenses administratives régulières.

SonicWall Hosted Email Security avec Capture Advance Threat Protection examine dynamiquement toutes les pièces jointes et URL suspectes, les analyse dans une sandbox multi-moteur, et bloque les fichiers ou URL dangereux avant qu'ils n'atteignent votre réseau. Capture ATP intègre notre technologie Real-Time Deep Memory Inspection (RTDMI™) en instance de brevet. En procédant à une inspection directement dans la mémoire, le moteur RTDMI détecte et bloque proactivement les menaces de masse de type zero-day et les logiciels malveillants inconnus. SonicWall Hosted Email Security avec Capture ATP assure une protection avancée des pièces jointes et des URL au moment du clic contre les ransomware et les attaques de phishing ciblées.

De même, il inclut l'analyse et la gestion avancées de la conformité et, en option, le chiffrement des e-mails, pour prévenir la fuite de données confidentielles et la violation des règles et sécuriser l'échange d'informations sensibles. Les règles peuvent être configurées au niveau de l'entreprise pour détecter les données sensibles dans le contenu et les pièces jointes des e-mails sortants et pour acheminer les e-mails en vue de leur approbation et de leur chiffrement. Les e-mails chiffrés peuvent être suivis pour confirmer l'heure à laquelle ils ont été reçus et ouverts.



Avantages :

- Protégez-vous contre les attaques de phishing ciblées et les e-mails frauduleux
- Stoppez les ransomware et les logiciels malveillants de type zero-day avant qu'ils n'atteignent votre boîte de réception
- Protégez les utilisateurs pour les empêcher de cliquer sur des liens malveillants sur n'importe quel appareil et de n'importe quel endroit avec une protection d'URL au moment du clic
- Sécurisez votre serveur de messagerie sur site, Office 365 et G Suite
- Bloquez les menaces émergentes grâce à des renseignements sur les menaces actualisés en temps réel
- Sécurisez vos données en appliquant des règles granulaires de prévention des pertes de données (DLP) et de conformité
- Bénéficiez d'une véritable mutualisation avec contrôle granulaire sur la gestion, la configuration, le reporting et l'identité de marque pour chaque client
- Bénéficiez de l'évolutivité dont vous avez besoin avec des tarifs d'abonnement prévisibles et zéro coût en amont
- Réduisez les frais généraux générés par les administrateurs et les fournisseurs de services grâce à la gestion et au reporting simplifiés
- Domptez la puissance du cloud et protégez la bande passante de votre réseau
- Garantisiez la remise des e-mails et l'absence d'impact sur la productivité lors de pannes planifiées ou non

Intuitif pour le destinataire, un e-mail de notification est envoyé dans sa boîte de réception avec les instructions pour se connecter simplement à un portail sécurisé permettant de lire et de télécharger l'e-mail en toute sécurité. Ce service est basé sur le Cloud et ne nécessite aucun logiciel client supplémentaire. Contrairement aux solutions concurrentes, les e-mails chiffrés sont accessibles et lisibles depuis les appareils mobiles ou ordinateurs portables.

De plus, le service inclut la configuration DMARC (Domain-based Message Authentication, Reporting and Conformance). Cette méthode efficace d'authentification des e-mails permet d'identifier les e-mails usurpés et de réduire les attaques de phishing évoluées, comme le spear-phishing, le whaling, l'arnaque au président et le BEC (Business Email Compromise). Elle permet aussi d'établir des rapports sur les sources et les expéditeurs d'e-mails en vue d'identifier et de bloquer les expéditeurs non autorisés qui falsifient les e-mails avec votre adresse, et ainsi de protéger votre marque.

SonicWall Hosted Email Security intègre plusieurs technologies antivirus pour offrir une sécurisation de messagerie optimale. SonicWall Capture Labs soumet chaque jour des millions d'e-mails à des évaluations et des tests rigoureux, puis réutilise cette analyse mise à jour en permanence, ce qui lui permet de garantir des résultats exceptionnels en termes de blocage de spam et de protection antivirus et antispyware.

En outre, avec la solution SonicWall Hosted Email Security, il n'y a aucun équipement à installer sur site, ce qui élimine les dépenses initiales en matériel et logiciel, et réduit le temps et les ressources nécessaires pour déployer et gérer la sécurisation de la messagerie. De même, un service hébergé n'engendre pas de mises à jour, de tâches de maintenance ni de frais supplémentaires pour le matériel et le logiciel. SonicWall se charge de tenir le service à jour, afin que vous ayez toujours accès aux dernières fonctionnalités et à l'offre de service la plus sûre, et que vous puissiez libérer votre personnel informatique pour qu'il se consacre à d'autres tâches. Avec SonicWall Hosted Email Security, les entreprises bénéficient d'une sécurisation de messagerie supérieure doublée d'une charge administrative moindre.

MSP et VAR

La solution SonicWall Hosted Email Security est également proposée aux fournisseurs de services gérés (MSP) et aux revendeurs à valeur ajoutée (VAR)

souhaitant élaborer pour leurs clients une offre différenciée et particulièrement rentable de sécurisation de messagerie de type SaaS (logiciel en tant que service) qui assure une protection supérieure, basée sur le Cloud, contre les menaces entrantes et sortantes, notamment les spams, le phishing, les menaces de type BEC, les ransomware et les logiciels malveillants, sans engendrer de frais initiaux ni de risque financier. Avec l'ajout d'une solution hébergée à sa gamme étendue de solutions de sécurisation de messagerie, SonicWall accroît les possibilités pour les AR et MSP de gagner en compétitivité et d'accroître leurs revenus, tout en limitant leurs risques, leurs charges administratives et leurs coûts réguliers.

Les MSP peuvent bénéficier d'une véritable mutualisation avec contrôle granulaire sur la gestion, la configuration, le reporting et l'identité de marque pour chaque client. Une page d'administration centralisée fournit une vue unique pour la gestion de tous les clients. Cette solution autorise une gestion granulaire permettant d'automatiser la configuration des licences et l'application des règles. En outre, grâce à un ensemble riche et puissant d'API RESTful, les MSP peuvent personnaliser la solution au fil des besoins de l'entreprise.

Enfin, SonicWall offre la continuité de messagerie afin de réduire l'impact des pannes planifiées ou non sur les serveurs de messagerie sur site ou les services cloud, tels qu'Office 365 et G Suite. Avec la continuité de messagerie, les MSP peuvent garantir la disponibilité des services 24x7 et respecter les strictes exigences des accords de niveau de service (SLA).

Fonctionnalités

Advanced Threat Protection : le service SonicWall Email Security Capture Advanced Threat Protection détecte et peut bloquer toute menace évoluée jusqu'à ce que l'analyse ait rendu son verdict. Ce service est la seule détection des menaces évoluées à offrir un mécanisme de sandboxing multicouche, comprenant des techniques de virtualisation et d'émulation complète du système Real-Time Deep Memory Inspection, pour analyser le code suspect dans les e-mails et protéger les clients face aux dangers croissants des menaces zero-day. Le service Capture ATP fournit une précision accrue grâce à une analyse dynamique des pièces jointes et des URL, à des fonctionnalités de reporting approfondi et à une expérience utilisateur optimisée.

Prise en charge améliorée d'Office 365 et de G Suite : le service SonicWall Hosted Email Security s'intègre à Office 365 et G Suite pour garantir une correspondance correcte et mappée des messages au sein d'un environnement mutualisé hébergé. De plus, Hosted Email Security prend en charge la liste d'autorisation automatique des adresses IP Office 365 et G Suite.

En outre, SonicWall Email Security réécrit toutes les URL intégrées pour bloquer les e-mails contenant des URL malveillantes ou de phishing, afin que les utilisateurs soient protégés au moment du clic sur n'importe quel appareil et à n'importe quel endroit.

Stoppez les attaques de phishing évoluées grâce aux techniques d'analyse avancées, comme la technologie anti-phishing de SonicWall, qui fait appel à une combinaison de méthodologies comme l'apprentissage automatique et l'analyse heuristique, de réputation et de contenu. Cette solution inclut aussi de puissantes normes d'authentification, comme SPF, DKIM et DMARC qui lui permettent de stopper les attaques par usurpation, le BEC (Business Email Compromise) et les e-mails frauduleux.

Protégez votre messagerie. Cette technologie fournit aussi une protection contre les attaques DHA (Directory Harvest Attack) et DoS (Denial of Service), et garantit la validation de l'expéditeur. Des techniques évoluées permettent aussi d'analyser le contenu des e-mails, notamment l'algorithme Support Vector Machine (SVM), le filtrage Adversarial Bayesian, l'analyse graphique et la détection de messages inintelligibles pour démasquer les menaces connues dissimulées et les nouvelles menaces. L'analyse des e-mails sortants préserve votre réputation en analysant – et bloquant – le trafic provenant de zombies et d'expéditeurs non autorisés, de même que les messages contenant des virus.

Bénéficiez de la protection la plus précise et la plus récente contre les nouvelles attaques de spam, tout en veillant à ce que le courrier légitime parvienne à destination grâce aux renseignements sur les menaces en temps réel provenant du réseau SonicWall Capture Threat Network, qui collecte des informations provenant de millions de sources. L'équipe de recherche SonicWall Capture Labs analyse les informations et réalise des tests rigoureux en vue d'établir des scores de réputation pour les expéditeurs et les contenus et d'identifier les nouvelles menaces en temps réel.

Bénéficiez d'une protection antivirus étendue englobant l'antivirus SonicWall GRID et des signatures antivirus haut de gamme, plus efficace que celle des solutions reposant sur une seule technologie antivirus. De plus, pour prévenir une infection par de nouveaux virus avant même que les mises à jour de signatures antivirus soient disponibles, des technologies prédictives identifient les e-mails contenant de nouveaux virus suspects et les mettent immédiatement en quarantaine, assurant ainsi la sécurité du réseau dans l'intervalle de temps séparant la déclaration d'un virus et la disponibilité de la nouvelle signature.

Gestion des règles de conformité et chiffrement des e-mails : conformez-vous aux exigences réglementaires en identifiant, surveillant et signalant les e-mails qui ne respectent pas les règles et directives de conformité (par ex. , HIPAA, SOX, GLBA et PCI DSS) ou les directives de l'entreprise sur les pertes de données. Grâce à la gestion des règles de conformité, vous pouvez configurer le filtrage des ID d'enregistrement pour rechercher avec facilité des informations prédéfinies et l'analyse des pièces jointes pour prévenir la divulgation non autorisée d'informations. Vous pouvez aussi choisir parmi des règles prédéfinies

pour satisfaire en toute simplicité aux exigences de conformité, notamment des dictionnaires prédéfinis pour garantir la protection des informations confidentielles. Vous pouvez en outre créer des boîtes de validation pour l'analyse et l'approbation des e-mails avant l'envoi et configurer le routage à base de règles des e-mails en vue de leur chiffrement, afin de sécuriser l'échange d'informations sensibles.

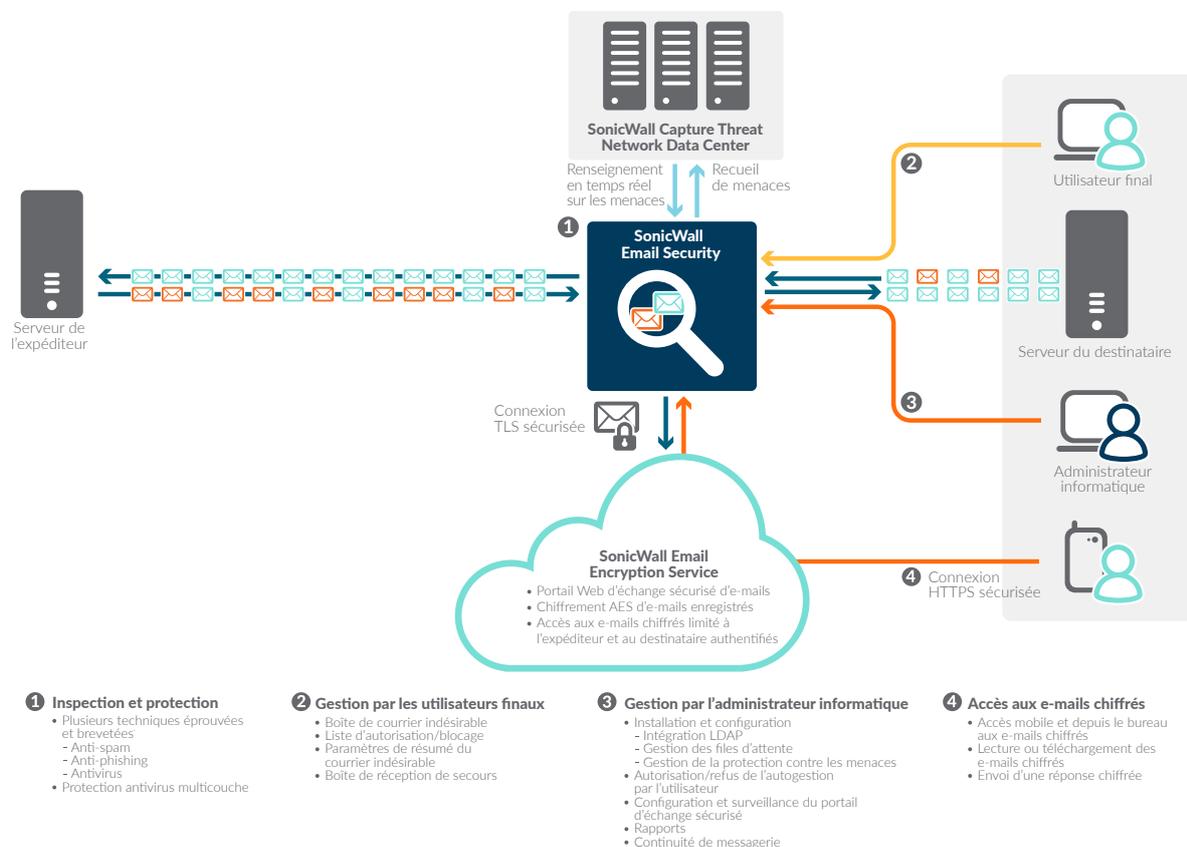
Disponibilité des services 24x7 avec continuité de messagerie : garantisiez la remise des e-mails et l'absence d'impact sur la productivité lors de pannes planifiées ou non des serveurs de messagerie sur site ou d'un fournisseur cloud, tel qu'Office 365 et G Suite. Lors des pannes, les utilisateurs peuvent accéder à une boîte de réception d'urgence pour rédiger des messages, les lire et y répondre. La mise en file d'attente des e-mails assure qu'aucun message n'est perdu en cas d'indisponibilité des serveurs de messagerie, et leur remise une fois que les serveurs sont à nouveau opérationnels.

Préservez la bande passante en bloquant les spams et les virus dans le cloud avant de livrer les e-mails légitimes au sein de l'infrastructure de messagerie du destinataire.

Simplifiez la gestion des spams en la déléguant en toute sécurité aux utilisateurs finaux. Ces derniers peuvent librement personnaliser la sévérité de leurs paramètres de détection des spams, tandis que les responsables informatiques conservent le contrôle nécessaire sur le niveau général de sécurité appliqué.

Gagnez en efficacité et en rentabilité en réduisant en amont vos coûts de déploiement ainsi que vos dépenses administratives régulières. Avec SonicWall Hosted Email Security, aucune installation matérielle ni logicielle sur site n'est nécessaire.

Simplifiez la vie des fournisseurs de services gérés avec une ouverture de session à partir d'un point unique pour les administrations via le Capture Security Center et grâce à la gestion mutualisée, à des options d'achat flexibles et à la configuration automatisée de plusieurs abonnés.



* Brevets (États-Unis) : 7 814 545 ; 7 343 624 ; 7 665 140 ; 7 653 698 ; 7 546 348

Fonctionnalités

Protection de messagerie complète en entrée et en sortie

Capture ATP (protection avancée des pièces jointes et des URL)	En option
Protection d'URL au moment du clic	Oui
Efficacité anti-spam	Oui
Réputation des adresses IP émettrices	Oui
Protection contre les DHA et DoS	Oui
Services de réputation Capture Labs	Oui
SonicWall Cloud Anti-Virus	Oui
Plusieurs technologies antivirus	Oui
Détection des URL malveillantes	Oui
Détection, classification et blocage du phishing	Oui
Détection des zombies, protection contre les inondations	Oui
Règles	Oui

Facilité d'administration

Gestion centralisée avec Capture Security Center	Oui
Gestion mutualisée	Oui
Prise en charge d'Office 365 et G Suite	Oui
Configuration et installation automatisées	Oui
Mises à jour automatiques des réputations	Oui
Mises à jour anti-spam automatiques	Oui
Mises à niveau et maintenance automatiques	Oui
Mises à jour automatiques des signatures antivirus	Oui
Personnalisation, programmation et envoi de rapports	Oui
Synchronisation LDAP automatique	Oui
Moteur de recherche rapide des messages	Oui

Simplicité pour les utilisateurs finaux

Authentification SMTP pour les e-mails entrants et sortants	Oui
Autorisation/refus de tous les contrôles d'utilisateurs finaux	Oui
Boîte de réception de secours	En option
Boîtes de courrier indésirable par utilisateur	Oui
Sévérité de l'anti-spam par utilisateur	Oui
Listes d'autorisation/blocage par utilisateur	Oui
Résumés du courrier indésirable en 15 langues	Oui
Détails de jugement	Oui

Caractéristiques système

Compatibilité avec tous les serveurs de messagerie SMTP	Oui
Prise en charge de l'authentification SMTP (SMTP AUTH)	Oui
Nombre illimité de domaines pris en charge	Oui
Continuité de messagerie	En option
Conservation des courriers indésirables pendant 15 jours	Oui
Mise en file d'attente des e-mails jusqu'à 7 jours	Oui

Caractéristiques (suite)

Règles et gestion de la conformité

Analyse des pièces jointes	Oui
Filtrage des ID d'enregistrement	Oui
Dictionnaires	Oui
Boîtes de validation/flux de travaux	Oui
Rapports de conformité	Oui

Service de chiffrement des e-mails pour Hosted Email Security – en option

Échange d'e-mails sécurisé à base de règles	Oui
Fonctionnement en natif sur les appareils mobiles (aucune appli requise)	Oui
Bouton complémentaire « Send Secure » pour Outlook	Oui
Chiffrement rapide des fichiers joints jusqu'à 100 Mo	Oui
Envoi de messages directement au destinataire sans qu'il n'ait besoin d'installer quoi que ce soit	Oui
Notification de message avec lien vers des comptes destinataires configurés automatiquement	Oui
Réponses automatiquement déchiffrées dans la boîte de réception de l'expéditeur	Oui
Suivi intégré de tous les messages et fichiers envoyés, reçus et ouverts	Oui
Personnalisation des e-mails chiffrés	Oui
Rapports et surveillance	Oui
500 Mo par société	Oui
Chiffrement standard et conforme : AES 256, TLS	Oui
Pas de clés à gérer ou risquant d'être égarées	Oui
Portail traduit en dix langues : anglais, français, italien, allemand, espagnol, japonais, portugais (Brésil), chinois simplifié, chinois traditionnel et coréen	Oui
Prise en charge d'Outlook 2010/2013/2016	Oui
SSAE 16, SAS 70 Type II & Fedramp Certified Data Center	Oui

Assistance et services

Support 24 h/24, 7 j/7 par téléphone et e-mail	Oui
Plusieurs centres de données	Oui

Abonnement	Référence
Service d'abonnement à Hosted Email Security	
Service d'abonnement à Hosted Email Security : 10 utilisateurs (1 an)	01-SSC-5030
Service d'abonnement à Hosted Email Security : 25 utilisateurs (1 an)	01-SSC-5033
Service d'abonnement à Hosted Email Security : 50 utilisateurs (1 an)	01-SSC-5036
Service d'abonnement à Hosted Email Security : 100 utilisateurs (1 an)	01-SSC-5039
Service d'abonnement à Hosted Email Security : 250 utilisateurs (1 an)	01-SSC-5042
Service d'abonnement à Hosted Email Security : 500 utilisateurs (1 an)	01-SSC-5045
Service d'abonnement à Hosted Email Security : 750 utilisateurs (1 an)	01-SSC-5057
Service d'abonnement à Hosted Email Security : 1 000 utilisateurs (1 an)	01-SSC-5048
Service d'abonnement à Hosted Email Security : 2 000 utilisateurs (1 an)	01-SSC-5051
Service Capture ATP pour Hosted Email Security	
Service Capture ATP pour Hosted Email Security : pack 10 utilisateurs - (1 an)	01-SSC-1650
Service Capture ATP pour Hosted Email Security : pack 25 utilisateurs - (1 an)	01-SSC-1653
Service Capture ATP pour Hosted Email Security : pack 50 utilisateurs - (1 an)	01-SSC-1656
Service Capture ATP pour Hosted Email Security : pack 100 utilisateurs - (1 an)	01-SSC-1659
Service Capture ATP pour Hosted Email Security : pack 250 utilisateurs - (1 an)	01-SSC-1838
Service Capture ATP pour Hosted Email Security : pack 500 utilisateurs - (1 an)	01-SSC-1511
Service Capture ATP pour Hosted Email Security : pack 750 utilisateurs - (1 an)	01-SSC-1514
Service Capture ATP pour Hosted Email Security : pack 1 000 utilisateurs - (1 an)	01-SSC-1517
Service Capture ATP pour Hosted Email Security : pack 2 000 utilisateurs - (1 an)	01-SSC-1520
Service Capture ATP pour Hosted Email Security : pack 5 000 utilisateurs - (1 an)	01-SSC-1523
Continuity for Hosted Email Security	
Continuity for Hosted Email Security : 10 utilisateurs - (1 an)	01-SSC-3068
Continuity for Hosted Email Security : 25 utilisateurs - (1 an)	01-SSC-3071
Continuity for Hosted Email Security : 50 utilisateurs - (1 an)	01-SSC-3074
Continuity for Hosted Email Security : 100 utilisateurs - (1 an)	01-SSC-3077
Continuity for Hosted Email Security : 250 utilisateurs - (1 an)	01-SSC-3080
Continuity for Hosted Email Security : 500 utilisateurs - (1 an)	01-SSC-3083
Continuity for Hosted Email Security : 750 utilisateurs - (1 an)	01-SSC-3086
Continuity for Hosted Email Security : 1 000 utilisateurs - (1 an)	01-SSC-3089
Continuity for Hosted Email Security : 2 000 utilisateurs - (1 an)	01-SSC-3092
Continuity for Hosted Email Security : 5 000 utilisateurs - (1 an)	01-SSC-3095
Service de chiffrement des e-mails pour Hosted Email Security	
Service de chiffrement des e-mails pour Hosted Email Security : 10 utilisateurs (1 an)	01-SSC-5078
Service de chiffrement des e-mails pour Hosted Email Security : 25 utilisateurs (1 an)	01-SSC-5081
Service de chiffrement des e-mails pour Hosted Email Security : 50 utilisateurs (1 an)	01-SSC-5084
Service de chiffrement des e-mails pour Hosted Email Security : 100 utilisateurs (1 an)	01-SSC-5087
Service de chiffrement des e-mails pour Hosted Email Security : 250 utilisateurs (1 an)	01-SSC-5091
Service de chiffrement des e-mails pour Hosted Email Security : 500 utilisateurs (1 an)	01-SSC-5094
Service de chiffrement des e-mails pour Hosted Email Security : 750 utilisateurs (1 an)	01-SSC-5097
Service de chiffrement des e-mails pour Hosted Email Security : 1 000 utilisateurs (1 an)	01-SSC-5104
Service de chiffrement des e-mails pour Hosted Email Security : 2 000 utilisateurs (1 an)	01-SSC-5107

Références pluriannuelles disponibles. Rendez-vous sur www.sonicwall.com

À propos de SonicWall

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les PME, les grandes entreprises et les agences gouvernementales du monde entier. S'appuyant sur les travaux de recherche des Capture Labs de SonicWall, nos solutions primées de détection et de prévention des intrusions en temps réel sécurisent plus d'un million de réseaux et leurs e-mails, applications et données dans plus de 215 pays et territoires. Ces entreprises peuvent ainsi fonctionner plus efficacement sans crainte pour leur sécurité. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur [Twitter](#), [LinkedIn](#), [Facebook](#) et [Instagram](#).