Appliances et logiciels Email Security

Protégez votre infrastructure contre les menaces de messagerie évoluées et la violation de règles de conformité grâce à des solutions puissantes et conviviales.

Les e-mails sont essentiels à la communication de votre entreprise, mais ils constituent aussi le premier vecteur de menace comme les ransomwares, le phishing, le BEC (Business Email Compromise), le spoofing, les spams et les virus. 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. Que votre organisation soit une PME en expansion, une grande entreprise distribuée ou un fournisseur de services gérés (MSP), vous avez besoin d'une solution économique de sécurisation de messagerie et de chiffrement. Évolutive, elle doit vous permettre d'augmenter facilement les capacités pour les unités et les domaines organisationnels et de déléguer la gestion.

Les appliances et logiciels SonicWall Email Security assurent une protection multicouche contre les menaces de messagerie entrantes et sortantes et la violation de règles de conformité en détectant les données sensibles dans le contenu et les pièces jointes des e-mails entrants et sortants et les URL, pour offrir une protection en temps réel contre les ransomwares, les attaques de phishing ciblées, le spoofing, les virus, les URL malveillantes, les zombies, les attaques DHA (Directory Harvest Attack), DoS (Denial of Service) et autres. Cette solution s'appuie sur les nombreuses techniques brevetées de détection des menaces de SonicWall et sur un réseau mondial, unique en son genre, d'identification et de surveillance des attaques.

Le service SonicWall Capture Advanced Threat Protection propose le meilleur sandboxing multimoteur et la technologie Real-time Deep Memory Inspection (RTDMI™) en instance de brevet, qui isolent les menaces inconnues détectées dans les pièces jointes et URL suspectes, et vous permettent de stocker les menaces évoluées avant qu'elles n'atteignent la boîte de réception de vos utilisateurs. La solution Email Security avec Capture ATP vous apporte une protection très efficace et réactive contre les attaques de type ransomware et zero-day.

La solution inclut également les normes DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) et DMARC (Domain-based Message Authentication, Reporting and Conformance), une méthode efficace d'authentification des e-mails qui permet d'identifier les e-mails usurpés, de réduire le spam et les attaques de phishing ciblées, 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 de protéger ainsi votre marque. De plus, elle prévient les fuites de données confidentielles et la violation des règles de conformité grâce à l'analyse et la gestion avancées de la conformité, notamment un service Cloud de chiffrement des e-mails intégré pour sécuriser l'échange d'informations sensibles.

L'administration de la solution Email Security est intuitive, rapide et simple. Vous pouvez déléguer en toute sécurité la gestion des spams aux utilisateurs finaux, tout en conservant le contrôle nécessaire sur les règles de sécurité appliquées. Vous pouvez aussi gérer en toute simplicité les comptes d'utilisateurs et de groupes grâce à une synchronisation multi-LDAP transparente. Dans les grands environnements distribués, la prise en charge de la mutualisation vous permet de charger des sous-administrateurs de gérer les paramètres au niveau de différentes unités organisationnelles (divisions de l'entreprise ou clients MSP, par ex.) au sein d'un seul et même déploiement Email Security.

Avantages

- Service Capture ATP de sécurisation de messagerie pour une protection contre les menaces évoluées de type ransomware et zero-day
- Techniques d'analyse avancées pour stopper les attaques de phishing ciblées, les e-mails frauduleux et le BEC (Business Email Compromise)
- Stoppez les nouvelles menaces grâce aux mises à jour de renseignements en temps réel sur les menaces de SonicWall Capture Labs
- Protégez votre messagerie grâce à de puissants services d'anti-spam et antivirus
- Sécurisez vos données en appliquant des règles granulaires de prévention des pertes de données (DLP) et de conformité
- Simplifiez la gestion grâce à l'automatisation intelligente, la délégation des tâches, un tableau de bord « en un coup d'œil » personnalisable et un reporting puissant
- Exploitez des options de déploiement flexibles et évolutives, notamment des appliances physiques renforcées, des appliances virtuelles robustes et de puissants logiciels pour Windows Server®

Fonctionnalités

Protection contre les menaces évoluées

Détectez et bloquez les menaces évoluées 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. Il comprend la protection avancée des URL qui analyse dynamiquement les URL intégrées. Les messages contenant des URL malveillantes sont donc bloqués et mis en quarantaine avant qu'ils n'atteignent la boîte de réception, ce qui évite aux utilisateurs de cliquer dessus et d'être attaqués. 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.

Protection contre les attaques ciblées

Stoppez les attaques de phishing évoluées grâce à la technologie anti-phishing de SonicWal, 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.

Renseignements en temps réel sur les menaces

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 informations sur les menaces en temps réel provenant du réseau SonicWall Capture Threat Network, qui collecte des informations provenant de millions de sources. 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.

Protection antivirus et anti-logiciels espions

Bénéficiez d'une protection antivirus et anti-logiciels espions à jour. La solution utilise les signatures des principales bases de données antivirus et la détection des URL malveillantes pour une protection multicouche supérieure à celle offerte par les solutions basées sur une seule technologie antivirus.

De plus, l'analyse prédictive vous permet de protéger votre réseau dans l'intervalle de temps séparant la déclaration d'un virus et la disponibilité de la nouvelle signature.

Automatisation intelligente, délégation des tâches et reporting puissant

Simplifiez la gestion grâce à l'automatisation intelligente, la délégation des tâches et un reporting puissant. Gérez automatiquement les adresses e-mail, les comptes et groupes d'utilisateurs. L'intégration à plusieurs serveurs LDAP est transparente. Déléguez en toute confiance la gestion des spams aux utilisateurs finaux avec le plug-in téléchargeable « Courrier indésirable » pour Outlook®, sachant que vous gardez le contrôle total. Localisez n'importe quel e-mail en quelques secondes avec le moteur de recherche rapide des messages. Le reporting centralisé (même en mode divisé) vous fournit des informations facilement personnalisables, précises et à l'échelle du système sur les types d'attaques, l'efficacité de la solution et la surveillance intégrée des performances. Les rapports sont disponibles aux formats PDF et JPEG.

Gestion des règles de conformité

Ce service complémentaire vous permet de vous conformer 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. Ce service d'abonnement permet aussi le routage à base de règles des e-mails en vue de leur approbation, archivage et chiffrement.

Chiffrement des e-mails

Ajoutez une structure puissante pour mettre fin aux fuites de données, gérer et appliquer les exigences de conformité et sécuriser les échanges d'e-mails sur terminaux mobiles pour les entreprises de toutes tailles.

Les e-mails chiffrés peuvent être suivis pour confirmer l'heure à laquelle ils ont été reçus et ouverts. 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 pas de logiciel client supplémentaire. Contrairement aux solutions concurrentes, les e-mails chiffrés sont accessibles et lisibles depuis les appareils mobiles ou ordinateurs portables.

Options de déploiement flexibles

Profitez d'un investissement à long terme évolutif en configurant votre solution dans une perspective de croissance et de redondance pour un coût initial minime. Vous pouvez déployer Email Security sous la forme d'une appliance hautes performances renforcée, d'un logiciel tirant parti de l'infrastructure existante ou d'une appliance virtuelle s'appuyant sur les ressources informatiques partagées pour optimiser l'utilisation, faciliter la migration et réduire les coûts d'investissement. Vous pouvez commencer avec un système unique et augmenter facilement la capacité pour passer à une architecture en mode divisé avec basculement, au gré de la croissance de votre entreprise. La prise en charge de la mutualisation permet des déploiements pour grandes entreprises et fournisseurs de services gérés comprenant de nombreux départements ou clients pour établir des unités organisationnelles avec un ou plusieurs domaines. Le déploiement peut être géré de manière centralisée, mais permet à une unité organisationnelle donnée de disposer de ses propres utilisateurs, sous-administrateurs, règles, boîtes de courrier indésirable, etc.

Options de déploiement pour SonicWall Email Security

L'architecture hautement flexible de SonicWall Email Security permet des déploiements au sein d'organisations qui nécessitent une solution de protection de messagerie distribuée extrêmement évolutive et redondante, pouvant être gérée de manière centralisée. SonicWall Email Security peut être déployé en configuration tout-en-un ou en mode divisé.

En mode divisé, les systèmes peuvent être configurés comme analyseur à distance ou centre de contrôle. Une installation typique en mode divisé comporte un ou plusieurs analyseurs à distance connectés à un centre de contrôle. L'analyseur à distance reçoit des e-mails d'un ou plusieurs domaines et utilise la gestion des connexions, le filtrage d'e-mails (anti-spam, anti-phishing et antivirus) et des techniques de régulation avancées pour acheminer les e-mails anodins au serveur de messagerie en aval. Le centre de contrôle gère de manière centralisée tous les analyseurs à distance et collecte et stocke le courrier indésirable de ces analyseurs. La gestion centralisée comprend le reporting et la surveillance de tous les systèmes connexes. Cette combinaison offre une évolutivité peu onéreuse et protège les e-mails entrants et sortants pour les entreprises en expansion. Grâce aux appliances virtuelles SonicWall Email Security, le mode divisé peut être entièrement déployé sur un ou plusieurs serveurs pour une efficacité d'échelle optimale.

1 Brevets U.S. n° 7 814 545 ; 7 343 624 ; 7 665 140 ; 7 653 698 ; 7 546 348

SONICWALL®

Caractéristiques

	APPLIANCE, APPLIANCE VIRTUELLE	WINDOWS SERVER®
Abonnement Advanced TotalSecure - Offre de protection avancée		
Comprend la protection avancée des pièces jointes et des URL de SonicWall Capture ATP en plus de l'abonnement TotalSecure	Oui	Oui
Abonnement TotalSecure - Offre de protection de base		
Comprend l'abonnement à Email Protection, le support dynamique 24X7, l'antivirus multicouche, la détection des URL malveillantes et des fonctionnalités d'abonnement pour la gestion de la conformité	Oui	Oui
Protection contre les ransomwares et les attaques zero-day – en option		
Service complémentaire de protection avancée des pièces jointes et des URL de SonicWall Capture ATP pour l'abonnement TotalSecure	Oui	Oui
Protection de messagerie complète en entrée et en sortie		
Efficacité anti-spam	Oui	Oui
Gestion des connexions avec réputation IP avancée	Oui	Oui
Détection, classification et blocage du phishing	Oui	Oui
Protection contre les DHA, DoS et NDR	Oui	Oui
Anti-spoofing avec prise en charge SPF, DKIM et DMARC	Oui	Oui
Règles valables pour des utilisateurs, groupes ou tous	Oui	Oui
MTA (Mail Transfer Agent) en mémoire pour un débit amélioré	Oui	Oui
Protection complète pour les messages entrants et sortants en un seul système	Oui	Oui
Facilité d'administration		
Installation	< 1 heure	< 1 heure
Gestion par semaine	< 10 min	< 10 min
Synchronisation multi-LDAP automatique des utilisateurs et groupes	Oui	Oui
Compatibilité avec tous les serveurs de messagerie SMTP	Oui	Oui
Prise en charge de l'authentification SMTP (SMPT AUTH)	Oui	Oui
Autorisation/refus des contrôles d'utilisateurs finaux	Oui	Oui
Personnalisation, programmation et envoi de plus de 30 rapports	Oui	Oui
Détails de jugement	Oui	Oui
Tableau de bord de gestion « en un coup d'œil » personnalisable	Oui	Oui
Moteur de recherche rapide des messages	Oui	Oui
Architecture évolutive en mode divisé	Oui	Oui
Clustering et clustering à distance	Oui	Oui
Simplicité pour les utilisateurs finaux		
Signature unique (SSO)	Oui	Oui
Boîtes de courrier indésirable par utilisateur, résumé du courrier indésirable avec option d'autorisation	Oui	Oui
Sévérité de l'anti-spam par utilisateur, listes d'autorisation/blocage	Oui	Oui
Abonnement à Email Protection avec support dynamique – requis		
Mises à jour automatiques de l'anti-spam, anti-phishing et antivirus Cloud SonicWall toutes les minutes	Oui	Oui
Support 24X7	Oui	Oui
RMA (remplacement matériel)	Oui	Oui
Mises à jour logiciel/firmware	Oui	Oui
Abonnement antivirus – en option		
Flux de signatures des bases de données antivirus leaders du marché	Oui	Oui
Antivirus SonicWall TimeZero	Oui	Oui
Détection de zombies	Oui	Oui
Abonnement Compliance – en option		
Gestion puissante des règles	Oui	Oui
Analyse des pièces jointes	Oui	Oui
Filtrage des ID d'enregistrement	Oui	Oui
Dictionnaires	Oui	Oui
Boîtes de validation/flux de travaux	Oui	Oui
Archivage des e-mails	Oui	Oui
Rapports de conformité	Oui	Oui
Abonnement Encryption – en option		
Possibilité d'abonnement à Compliance, plus chiffrement et échange sécurisé des e-mails sur la base de règles	Oui	Oui

Spécifications système

APPLIANCES EMAIL SECURITY	5000	7000	9000
Nombre de domaines	Illimité		
Système d'exploitation	Appliance avec SE Linux renforcé SonicWall		
Châssis rackable	1 U	1 U	1 U
Processeur(s)	Celeron G1820	i3-4330	E3-1275 v3
Mémoire vive	8 Go	16 Go	32 Go
Disque dur	500 G0	1 To	1 To
Matrice de disques redondante (RAID)	–	RAID 1	RAID 5
Lecteurs remplaçables à chaud	Non	Oui	Oui
Alimentation redondante	Non	Non	Oui
Mode sans échec Flash	Oui	Oui	Oui
Dimensions	43,18 x 41,59 x 4,44 cm/ 17,0 x 16,4 x 1,7 in	43,18 x 41,59 x 4,44 cm/ 17,0 x 16,4 x 1,7 in	69,9 x 48,3 x 8,9 cm/ 27,5 x 19,0 x 3,5 in
Poids	7,26 kg/16 lb	7,26 kg/16 lb	22,7 kg/50,0 lb
Poids DEEE	7,37 kg/16 lb	7,37 kg/16 lb	22,2 kg/48,9 lb
Consommation (watts)	46	48	158
BTU	155	162	537
MTBF à 25 °C en heures	130 919	150 278	90 592
MTBF à 25 C en années	14,9	17,2	10,3
Logiciel Email Security			
Nombre de domaines	Illimité		
Système d'exploitation	Microsoft Hyper-V Server 2012 (64 bits) ou version ultérieure Windows Server 2008 R2 ou version ultérieure (64 bits uniquement)		
Unité centrale	Processeur Intel ou AMD 64 bits		
Mémoire vive	Configuration minimum 8 Go		
Disque dur	Configuration minimum 160 Go		
Appliance virtuelle Email Security			
Hyperviseur	ESXi™ et ESX™ (version 5.0 ou plus récente)		
Système d'exploitation installé	8 Go (extensible)		
Mémoire allouée	4 Go		
Taille de disque de l'appliance	160 Go (extensible)		
Guide de compatibilité matérielle VMware	http://www.vmware.com/resources/compatibility/search.php		

Informations de commande de SonicWall Email Security

Appliances SonicWall Email Security

N° de référence	Produit
01-SSC-7605	SonicWall Email Security Appliance 9000
01-SSC-7604	SonicWall Email Security Appliance 7000
01-SSC-7603	SonicWall Email Security Appliance 5000
01-SSC-6636	Logiciel SonicWall Email Security
01-SSC-7636	Appliance virtuelle SonicWall Email Security

Abonnements à SonicWall Email Security

N° de référence	Abonnement
Abonnement à SonicWall Email Protection	
01-SSC-6669	Abonnement SonicWall Email Protection et support 24X7 25 utilisateurs – 1 serveur (1 an)
01-SSC-6678	Abonnement SonicWall Email Protection et support 24X7 1 000 utilisateurs – 1 serveur (1 an)
01-SSC-6730	Abonnement SonicWall Email Protection et support 24X7 10 000 utilisateurs – 1 serveur (1 an)
Abonnement à SonicWall Email Anti-Virus	
01-SSC-6759	SonicWall Email Anti-Virus 25 utilisateurs – 1 serveur (1 an)
01-SSC-6768	SonicWall Email Anti-Virus 1 000 utilisateurs – 1 serveur (1 an)
01-SSC-7562	SonicWall Email Anti-Virus 10 000 utilisateurs – 1 serveur (1 an)
Abonnement à SonicWall Email Encryption	
01-SSC-7427	Service SonicWall Email Encryption 25 utilisateurs (1 an)
01-SSC-7471	Service SonicWall Email Encryption 1 000 utilisateurs (1 an)
01-SSC-7568	Service SonicWall Email Encryption 10 000 utilisateurs (1 an)
Abonnement à SonicWall Email Compliance	
01-SSC-6639	Service SonicWall Email Compliance 25 utilisateurs – 1 serveur (1 an)
01-SSC-6648	Service SonicWall Email Compliance 1 000 utilisateurs – 1 serveur (1 an)
01-SSC-6735	Service SonicWall Email Compliance 10 000 utilisateurs – 1 serveur (1 an)
Abonnement à SonicWall TotalSecure Email	
01-SSC-7399	Abonnement SonicWall TotalSecure Email 25 utilisateurs (1 an)
01-SSC-7398	Abonnement SonicWall TotalSecure Email 1 000 utilisateurs (1 an)
01-SSC-7405	Abonnement SonicWall TotalSecure Email 10 000 utilisateurs (1 an)
Module complémentaire Capture ATP pour l'abonnement à TotalSecure	
01-SSC-1526	Capture ATP pour l'abonnement SonicWall TotalSecure Email 25 utilisateurs (1 an)
01-SSC-1874	Capture ATP pour l'abonnement SonicWall TotalSecure Email 1 000 utilisateurs (1 an)
01-SSC-1883	Capture ATP pour l'abonnement SonicWall TotalSecure Email 10 000 utilisateurs (1 an)
Abonnement à SonicWall Advanced TotalSecure Email (Capture ATP inclus)	
01-SSC-1886	Abonnement SonicWall Advanced TotalSecure Email 25 utilisateurs (1 an)
01-SSC-1904	Abonnement SonicWall Advanced TotalSecure Email 1 000 utilisateurs (1 an)
01-SSC-1913	Abonnement SonicWall Advanced TotalSecure Email 10 000 utilisateurs (1 an)

Offres de l'appliance SonicWall Email Security et abonnements disponibles en packs de 25, 50, 100, 250, 500, 1 000, 2 000, 5 000 et 10 000 utilisateurs, pour 1, 2 ou 3 ans. Support également disponible en formule 8X5. Veuillez contacter votre revendeur SonicWall pour obtenir la liste complète des références.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-KJ-MKTG3341