SONICWALL

Appareils et logiciels de sécurité de la messagerie électronique

Protégez votre infrastructure contre les menaces avancées à la messagerie électronique et les violations de la conformité grâce à des solutions puissantes et simples à utiliser

La messagerie électronique est un composant essentiel de la communication de l'entreprise, mais elle est aussi le premier vecteur d'attaque pour les menaces telles que ransomwares, phishing, BEC (Business Email Compromise), spoofing, spam et 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 petite ou moyenne entreprise (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 appareils et logiciels de sécurité de la messagerie électronique de SonicWall offrent une protection multicouche contre les menaces et les violations de la conformité des e-mails entrants et sortants en analysant tout le contenu des e-mails entrants et sortants, les URL et les pièces jointes pour identifier les données sensibles, en fournissant 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), le déni de service (DoS) et d'autres attaques. La solution exploite plusieurs techniques brevetées de détection des menaces de SonicWall et un réseau unique d'identification et de surveillance des attaques dans le monde entier.

Le service Capture Advanced Threat Protection de SonicWall offre une technologie sandbox multimoteur de pointe, avec la technologie Real-Time Deep Memory Inspection (RTDMI™) en instance de brevet, pour isoler les menaces inconnues trouvées dans les pièces jointes et URL de fichiers suspects, afin que vous puissiez arrêter les menaces avancées avant qu'elles n'atteignent les boîtes de réception de vos utilisateurs. Email Security combiné à Capture ATP vous offre une défense très efficace et réactive contre les ransomwares et les attaques zero-day.

La solution comprend également de puissantes normes d'authentification des e-mails, comme Domain-based Message Authentication, DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework), Reporting and Conformance (DMARC), permettant d'identifier les e-mails falsifiés, de réduire les spams et les attaques de phishing ciblées telles que 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. En outre, elle empêche les fuites de données confidentielles et les infractions réglementaires grâce à une analyse et une gestion avancées de la conformité, y compris un service cloud intégré de chiffrage des e-mails pour garantir l'échange sécurisé de données 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.

[1] Brevets américains 7,814,545 ; 7,343,624 ; 7,665,140 ; 7,653,698 ; 7,546,348

Avantages

- Empêchez les ransomwares et les logiciels malveillants zero-day d'atteindre votre boîte de réception grâce à Capture Advanced Threat Protection
- 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
- Techniques d'analyse avancées pour stopper les attaques de phishing ciblées, la fraude par e-mail et la compromission des e-mails professionnels (BEC)
- Bloquez les nouvelles menaces grâce aux mises à jour en temps réel des renseignements sur les menaces des Capture Labs de SonicWall
- Protégez votre messagerie électronique grâce à un puissant anti-spam et antivirus
- Protégez 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 personnalisable en un coup d'œil et un reporting robuste
- Tirez parti des options de déploiement flexibles et évolutives, notamment des appareils physiques durcis, des appareils virtuels robustes et du puissant logiciel Windows Server®

Fonctionnalités

Advance Threat Protection

Détecter et bloquer les menaces avancées jusqu'au 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 comprend une protection avancée des URL qui analyse de manière dynamique les adresses URL incorporées, afin de bloquer et de mettre en quarantaine les messages comportant des adresses URL malveillantes avant qu'ils n'arrivent dans la boîte de réception ; ainsi les utilisateurs ne cliquent jamais dessus et ne compromettent pas leur compte. Le service Capture ATP fournit une précision accrue grâce à une analyse des pièces jointes et des URL, à des fonctionnalités de reporting approfondi et à une expérience utilisateur optimisée.

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.

Certaines organisations et agences gouvernementales ne peuvent pas utiliser des techniques basées sur le cloud pour l'inspection des fichiers, comme Capture ATP, pour des raisons de conformité ou de latence. Intégrez votre appareil Email Security avec l'appareil SonicWall Capture Security (CSa) pour examiner les fichiers suspects arrivant par e-mail dans votre propre centre de données. CSa peut être référencé selon l'adresse IP ou FQDN, ce qui en fait une excellente ressource pour la prévention des menaces.

Protection contre les attaques ciblées

La technologie anti-phishing de SonicWall fait appel à une combinaison de méthodologies comme l'apprentissage automatique et l'analyse heuristique, de réputation et de contenu pour stopper les attaques de phishing évoluées. 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.

Renseignement 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. Les SonicWall Capture Labs analysent les informations et réalisent 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

Mettez à jour votre protection antivirus et anti-logiciels espions. La solution utilise des signatures provenant de bases de données antivirus de pointe et de détections d'URL malveillantes pour une protection multicouche supérieure à celle fournie par des solutions reposant sur une technologie antivirus unique.

En outre, l'analyse prédictive vous permet de protéger votre réseau à partir du moment où un nouveau virus apparaît jusqu'au moment où une mise à jour de signature antivirus est disponible.

Automatisation intelligente, délégation de tâches et reporting robuste

Simplifiez la gestion grâce à l'automatisation intelligente, la délégation des tâches et un reporting robuste. Gérez automatiquement les adresses e-mail, les comptes et les groupes d'utilisateurs. Intégration fluide avec plusieurs serveurs LDAP. Confiez en toute confiance la gestion des spams aux utilisateurs finaux grâce au plug-in d'Outlook® téléchargeable du bouton de courrier indésirable, tout en conservant un contrôle total. Localisez n'importe quel e-mail en quelques secondes grâce au moteur de recherche rapide de messages. Le reporting centralisé (même en mode divisé) vous donne des informations facilement personnalisables, à l'échelle du système et granulaires sur les types d'attaques, l'efficacité de la solution et le suivi des performances intégré. En outre, les rapports sont disponibles aux formats PDF et JPEG.

Gestion des règles de conformité

Ce service complémentaire permet de se conformer aux exigences réglementaires en vous aidant à identifier, surveiller et signaler 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. Le service d'abonnement permet également d'acheminer du courrier en fonction des règles pour approbation, archivage et chiffrement.

Chiffrement des e-mails

Ajoutez un cadre puissant pour stopper les fuites de données, gérer et faire respecter les exigences liées à la conformité et fournir un échange sécurisé de courrier électronique mobile compatible pour les organisations 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. Le service est basé sur le cloud sans logiciel client supplémentaire nécessaire, et contrairement aux solutions concurrentes, le courrier électronique chiffré peut être consulté et lu depuis des appareils mobiles ou des ordinateurs portables.

Options de déploiement flexibles

Gagnez en valeur évolutive et durable en configurant votre solution pour la croissance et la redondance avec des coûts initiaux minimes. Vous pouvez déployer Email Security sous la forme d'un appareil hautes performances renforcé, d'un logiciel exploitant une infrastructure existante ou d'un appareil virtuel s'appuyant sur les ressources informatiques partagées pour optimiser l'utilisation, faciliter la migration et réduire les coûts d'investissement. Commencez avec un système unique, puis à mesure que votre entreprise se développe, ajoutez des capacités et passez à une architecture en mode divisé activée par basculement. La prise en charge par mutualisation permet aux grandes entreprises ou aux fournisseurs de services gérés de déployer plusieurs services ou clients pour établir des unités organisationnelles avec un ou plusieurs domaines. Le déploiement peut être géré de manière centralisée, mais permet

toujours à une unité organisationnelle donnée d'avoir ses propres utilisateurs, sous-administrateurs, règles, courrier indésirable, entre autres.

Options de déploiement de SonicWall Email Security

L'architecture très flexible de SonicWall Email Security permet des déploiements dans des organisations qui nécessitent une solution de protection des e-mails hautement évolutive, redondante et distribuée pouvant être gérée de manière centralisée. SonicWall Email Security peut être déployé en mode tout-en-un ou en mode divisé.

En mode divisé, les systèmes peuvent être configurés comme un analyseur à distance ou un centre de contrôle. Dans une configuration typique en mode divisé, un ou plusieurs analyseurs à distance sont connectés à un centre de contrôle. L'analyseur à distance reçoit des e-mails d'un ou plusieurs domaines et applique la gestion des connexions, le filtrage des e-mails (anti-spam, anti-phishing et antivirus) et des techniques de règles avancées pour fournir des e-mails légitimes au serveur de messagerie en aval. Le centre de contrôle gère de manière centralisée tous les analyseurs à distance et collecte et stocke les courriers indésirables des analyseurs à distance. La gestion centralisée comprend le reporting et la surveillance de tous les systèmes associés. Ce paradigme permet à la solution de réduire les coûts et de protéger les e-mails entrants et sortants pour les entreprises en croissance. En utilisant les appareils virtuels de SonicWall Email Security, le mode divisé peut être entièrement déployé sur un ou plusieurs serveurs pour une efficacité d'échelle optimale.

Fonctionnalités

	APPAREIL, APPAREIL VIRTUEL	WINDOWS SERVER®
Abonnement Advanced Total Secure – Offre de protection avancée		
Inclut la protection avancée des pièces jointes et URL Capture ATP de SonicWall, en plus de l'abonnement Total Secure	Oui	Oui
Protection d'URL au moment du clic	Oui	Oui
Abonnement Total Secure – Offre de protection de base		
Inclut un abonnement dynamique 24 h/24 et 7 j/7 à la protection des e-mails ainsi que des fonctionnalités d'abonnement à l'antivirus multicouche, à la détection d'URL malveillantes et à la gestion de la conformité	Oui	Oui
Protection contre les ransomwares et attaques zero-day – facultatif		
Complément de la protection avancée des pièces jointes et URL Capture ATP de SonicWall pour l'abonnement Total Secure	Oui	Oui
Protection de messagerie complète en entrée et en sortie		
Anti-spam	Oui	Oui
Gestion de la connexion avec une 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 assistance pour SPF, DKIM et DMARC	Oui	Oui
Règles pour l'utilisateur, le groupe, tous	Oui	Oui
Agent de transfert de messages en mémoire (MTA) pour un meilleur débit	Oui	Oui
Facilité d'administration		
Installation	Moins d'une heure	Moins d'une heure
Gestion par semaine	Moins de 10 min	Moins de 10 min
Synchronisation automatique multi-LDAP pour les utilisateurs, les 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 personnalisable en un coup d'œil	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		
Authentification unique	Oui	Oui
Courrier indésirable par utilisateur, résumé du courrier indésirable pouvant faire l'objet d'une action	Oui	Oui
Agressivité anti-spam par utilisateur, bloquer/autoriser les listes	Oui	Oui
Abonnement à la protection des e-mails avec assistance dynamique – obligatoire		
Mises à jour automatiques antivirus, anti-spam et anti-phishing du cloud de SonicWall toutes les minutes	Oui	Oui
Support 24 h/24, 7 j/7	Oui	Oui
RMA (remplacement d'appareil)	Oui	Oui
Mises à jour du logiciel/micrologiciel	Oui	Oui
Abonnement antivirus – facultatif		
Flux de signatures provenant de bases de données antivirus de pointe	Oui	Oui
Antivirus cloud de SonicWall	Oui	Oui
Détection de zombies	Oui	Oui
Abonnement conformité – facultatif		
Gestion rigoureuse 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 au chiffrement – facultatif		
Capacités d'abonnement de conformité, chiffrement des e-mails imposé par la règle et échange sécurisé d'e-mails	Oui	Oui

Caractéristiques du système

PÉRIPHÉRIQUES DE SÉCURITÉ DE LA MESSAGERIE	5000	7000	9000
Domaines		Sans restriction	
Système d'exploitation		Appareil OS Linux SonicWall durci	
Châssis de montage sur rack	1RU	1RU	1RU
CPU(s)	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 Go	16 Go	32 Go
Disque dur	500 Go	1 To	1 To
Réseau de disques redondants (RAID)	—	RAID 1	RAID 5
Disques durs échangeables à chaud	Non	Oui	Oui
Alimentation électrique redondante	Non	Non	Oui
Flash mode sans échec	Oui	Oui	Oui
Dimensions	43,18 x 41,59 x 4,44 cm/ 17,0 x 16,4 x 1,7 po	43,18 x 41,59 x 4,44 cm/ 17,0 x 16,4 x 1,7 po	69,9 x 48,3 x 8,9 cm/ 27,5 x 19,0 x 3,5 po
Poids	7,26 kg/16 lb	7,26 kg/16 lb	22,7 kg/50 lb
Poids DEEE	7,37 kg/16 lb	22,2 kg/16 lb	22,2 kg/48,9 lb
Consommation électrique (watts)	46	48	158
BTUs	155	162	537
MTBF @25C en heures	130 919	150 278	90 592
MTBF @25C en années	14,9	17,2	10,3
LOGICIEL EMAIL SECURITY			
Domaines		Sans restriction	
Système d'exploitation		Microsoft Hyper-V Server 2012 (64 bits) ou supérieur Windows Server 2008 R2 ou supérieur, x64 bits uniquement	
CPU		Processeur Intel ou AMD 64 bits	
RAM		8 Go de configuration minimum	
Disque dur		160 Go de configuration minimum	
APPAREIL VIRTUEL EMAIL SECURITY			
Hyperviseur		ESXi™ et ESX™ (version 5.0 et ultérieure)	
Système d'exploitation installé		8 Go (extensible)	
Mémoire allouée		4 Go	
Taille du disque de l'appareil		160 Go (extensible)	
Guide de compatibilité de matériel VMware		http://www.vmware.com/resources/compatibility/search.php	

Partenaire de services

Besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Le programme avancé Partenaire de services SonicWall a pour objectif de vous fournir des services professionnels de classe mondiale. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

Informations de commande de SonicWall Email Security

Appareils SonicWall Email Security

Produit	Référence
Appareils SonicWall Email Security 9000	01-SSC-7605
Appareils SonicWall Email Security 7000	01-SSC-7604
Appareils SonicWall Email Security 5000	01-SSC-7603
Logiciel SonicWall Email Security	01-SSC-6636
Appareil virtuel SonicWall Email Security	01-SSC-7636

Abonnements SonicWall Email Security

Abonnement	Référence
Abonnement à SonicWall Email Protection	
Abonnement à SonicWall Email Protection et assistance 24 h/24, 7 j/7, 25 utilisateurs – 1 serveur (1 an)	01-SSC-6669
Abonnement à SonicWall Email Protection et assistance 24 h/24, 7 j/7, 1 000 utilisateurs – 1 serveur (1 an)	01-SSC-6678
Abonnement à SonicWall Email Protection et assistance 24 h/24, 7 j/7, 10 000 utilisateurs – 1 serveur (1 an)	01-SSC-6730
Abonnement à SonicWall Email AntiVirus	
SonicWall Email AntiVirus, 25 utilisateurs – 1 serveur (1 an)	01-SSC-6759
SonicWall Email AntiVirus, 1 000 utilisateurs – 1 serveur (1 an)	01-SSC-6768
SonicWall Email AntiVirus, 10 000 utilisateurs – 1 serveur (1 an)	01-SSC-7562
Abonnement SonicWall Email Encryption	
SonicWall Email Encryption Service, 25 utilisateurs (1 an)	01-SSC-7427
SonicWall Email Encryption Service, 1 000 utilisateurs (1 an)	01-SSC-7471
SonicWall Email Encryption Service, 10 000 utilisateurs (1 an)	01-SSC-7568
Abonnement à SonicWall Email Compliance	
SonicWall Email Compliance Service, 25 utilisateurs – 1 serveur (1 an)	01-SSC-6639
SonicWall Email Compliance Service, 1 000 utilisateurs – 1 serveur (1 an)	01-SSC-6648
SonicWall Email Compliance Service, 10 000 utilisateurs – 1 serveur (1 an)	01-SSC-6735
Abonnement SonicWall TotalSecure Email	
Abonnement SonicWall TotalSecure Email, 25 utilisateurs (1 an)	01-SSC-7399
Abonnement SonicWall TotalSecure Email, 1 000 utilisateurs (1 an)	01-SSC-7398
Abonnement SonicWall TotalSecure Email, 10 000 utilisateurs (1 an)	01-SSC-7405
Complément Capture ATP pour l'abonnement à TotalSecure Email	
Capture ATP pour l'abonnement à TotalSecure Email, 25 utilisateurs (1 an)	01-SSC-1526
Capture ATP pour l'abonnement à TotalSecure Email, 1 000 utilisateurs (1 an)	01-SSC-1874
Capture ATP pour l'abonnement à TotalSecure Email, 10 000 utilisateurs (1 an)	01-SSC-1883
Abonnement à SonicWall Advanced TotalSecure Email (Capture ATP inclus)	
Abonnement SonicWall Advanced TotalSecure Email, 25 utilisateurs (1 an)	01-SSC-1886
Abonnement SonicWall Advanced TotalSecure Email, 1 000 utilisateurs (1 an)	01-SSC-1904
Abonnement SonicWall Advanced TotalSecure Email, 10 000 utilisateurs (1 an)	01-SSC-1913

Les offres groupées et abonnements aux appareils SonicWall Email Security sont disponibles en packs de 25, 50, 100, 250, 500, 1 000, 2 000, 5 000 et 10 000 utilisateurs et avec des options sur 1, 2 et 3 ans. L'assistance est également disponible en option 8X5. Veuillez contacter votre revendeur SonicWall pour obtenir la liste complète des références

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.

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

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150