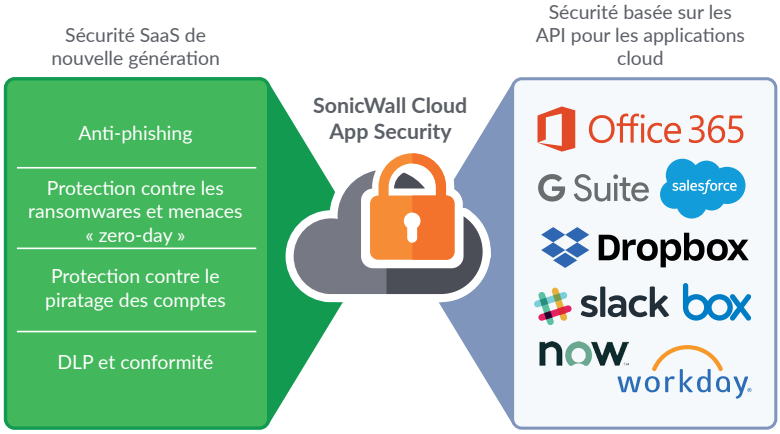
SONICWALL

SonicWall Cloud App Security

La solution SonicWall Cloud App Security fournit une sécurité de nouvelle génération pour les applications SaaS, comme Office 365 et G Suite, en protégeant les e-mails, données et identifiants de connexion des utilisateurs des menaces avancées, tout en garantissant la conformité dans le Cloud. Si vous migrez dans le Cloud, SonicWall fournit la meilleure sécurité basée sur les API de sa catégorie avec un faible coût total de possession, des dépenses minimes pour le déploiement et une expérience utilisateur fluide.



Visibilité : Identifiez tous les services cloud (à la fois autorisés et non autorisés) utilisés par les employés d'une entreprise. Cela englobe la visibilité du trafic est-ouest (de cloud à cloud) car les utilisateurs peuvent s'authentifier sur des applications non autorisées à l'aide d'une solution informatique autorisée, comme Office 365.

Sécurité de la messagerie électronique de nouvelle génération : Étant donné que la messagerie électronique devient l'application SaaS la plus utilisée, la protection de ce vecteur de menace prisé est indispensable à la sécurité SaaS. La solution comprend une technologie sandbox des pièces jointes, une protection avancée des URL et une protection contre les attaques d'entreprises par e-mails frauduleux (BEC).

Protection avancée contre les menaces : Prévenez la propagation des logiciels malveillants via les applications cloud, comme OneDrive, Box et Dropbox, grâce à une détection en temps réel des menaces connues et via la technologie sandbox Capture ATP pour les attaques « zero day » et les menaces inconnues.

Sécurité des données : Appliquez des politiques de sécurité orientées données en proposant des contrôles d'accès granulaires et en prévenant le téléchargement des fichiers sensibles ou confidentiels. La solution intègre des outils de politiques basées sur des rôles, ainsi que des technologies de classification des données et de prévention des fuites pour surveiller l'activité des utilisateurs et bloquer ou limiter l'accès.

Conformité : La solution collecte un système complet de traçabilité de chaque action, y compris des événements en temps réel et passés et fournit de simples modèles DLP pour appliquer les mesures de contrôle en temps réel des règles et la conformité réglementaire.

Avantages :

Sécurité de la messagerie électronique de nouvelle génération

- Bloquez les ransomwares, les attaques de type « zero-day » et les e-mails de phishing ciblés avant qu'ils n'atteignent la boîte de réception des utilisateurs
- Bénéficiez d'une protection avancée contre les menaces avec une technologie sandbox des pièces jointes et une protection avancée des URL
- Analysez les messages électroniques entrants, sortants et internes dans Office 365 et G Suite
- Bloquez les attaques par usurpation d'identité à l'aide de l'apprentissage automatique et de l'intelligence artificielle (IA)
- Empêchez tout e-mail malveillant d'atteindre les boîtes de réception des utilisateurs après leur envoi

Sécurité SaaS de nouvelle génération (CASB)

- Bénéficiez d'une visibilité et d'un contrôle granulaires sur les solutions informatiques autorisées et le « shadow IT »
- Obtenez une couverture complète pour le trafic de l'utilisateur vers le cloud, et du cloud vers le cloud
- Empêchez les téléchargements de données sensibles et le partage non autorisé de fichiers
- Configurez des règles de sécurité des données cohérentes sur toutes les applications autorisées
- Protégez-vous contre le piratage de compte (ATO), les menaces internes et les identifiants compromis
- Bloquez la propagation des ransomwares et des attaques malveillantes de type « zero-day » dans le cloud
- Appliquez les règles de conformité réglementaire en utilisant de simples modèles DLP
- Identifiez les infractions et les failles de sécurité en analysant l'historique d'événements, ainsi que les événements en temps réel

Simplicité et rentabilité de la sécurité

- Fournissez une expérience utilisateur fluide pour l'accès depuis n'importe quel appareil et site
- Supprimez les points de défaillance, les problèmes de latence et le besoin de rediriger le trafic via un proxy
- Automatisez la découverte des applications cloud lors du déploiement des pare-feu de nouvelle génération SonicWall
- Atteignez un faible coût total de possession avec un déploiement rapide et une simplicité d'utilisation

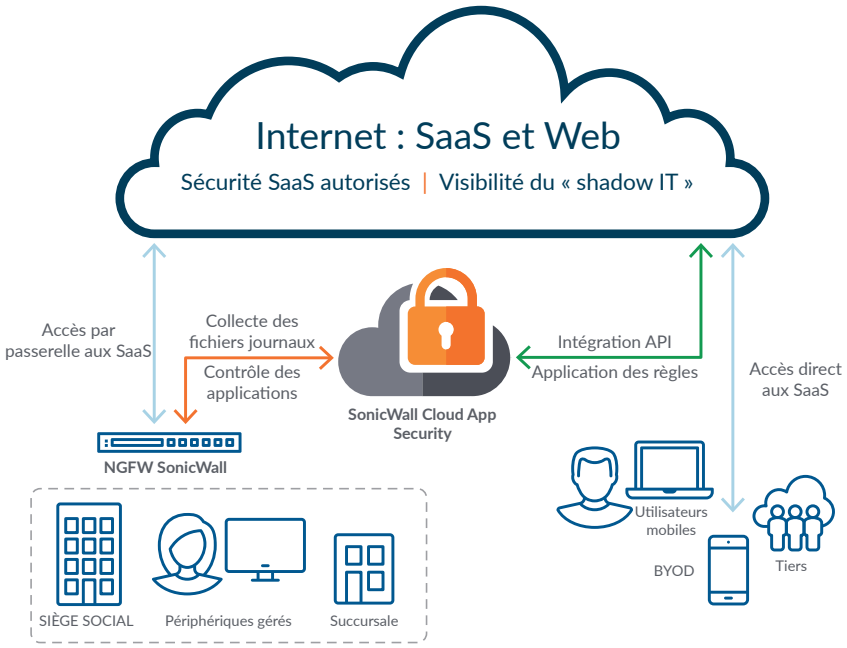
Aperçu de la solution

Description de la solution SonicWall

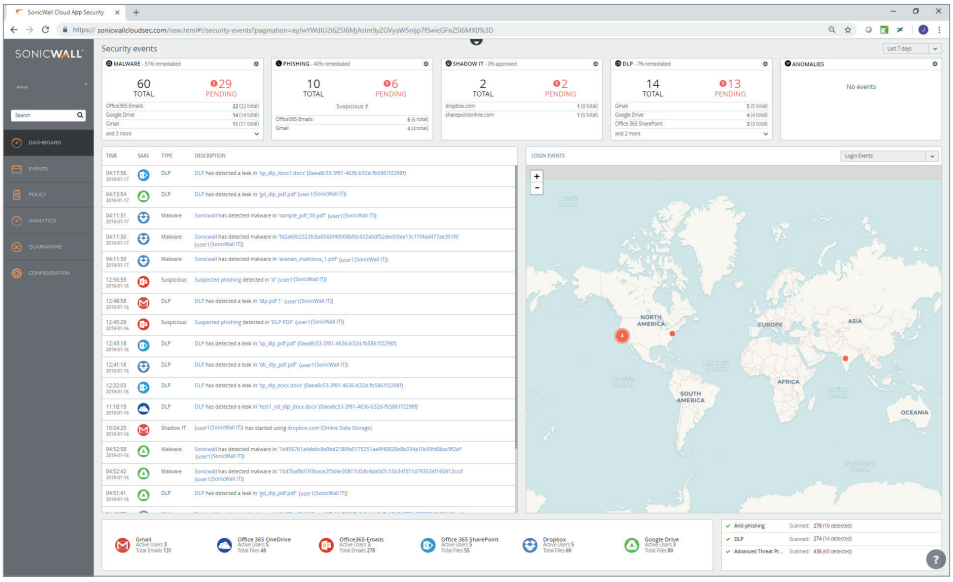
La solution SonicWall Cloud App Security permet une analyse hors bande du trafic vers les applications SaaS autorisées et interdites à l'aide des API et de l'analyse des fichiers journaux du trafic.

La solution s'intègre de manière fluide aux applications SaaS autorisées en utilisant des API natives, en fournissant des fonctionnalités CASB : visibilité, protection avancée contre les menaces, prévention contre la perte de données et la conformité. Lorsqu'elle est déployée avec un pare-feu de nouvelle génération (NGFW) SonicWall, la solution Cloud App Security propose une visibilité et un contrôle du « shadow IT » pour l'utilisation du cloud sur le réseau.

La solution permet aux départements informatiques de déployer des applications SaaS sans compromettre la sécurité ni la conformité. Les administrateurs peuvent configurer des politiques cohérentes sur toutes les applications SaaS déployées au sein de l'organisation depuis une unique console. Utilisez des modèles de rapports pour la DLP et la conformité afin de remédier rapidement aux failles de sécurité et de configurer les politiques personnalisées pour satisfaire aux besoins commerciaux et réglementaires. Que vous ayez quelques centaines d'utilisateurs ou des centaines de milliers d'employés répartis dans le monde entier, la solution peut s'adapter pour répondre à vos besoins sans que vous n'ayez besoin d'installer ni de gérer du matériel informatique.



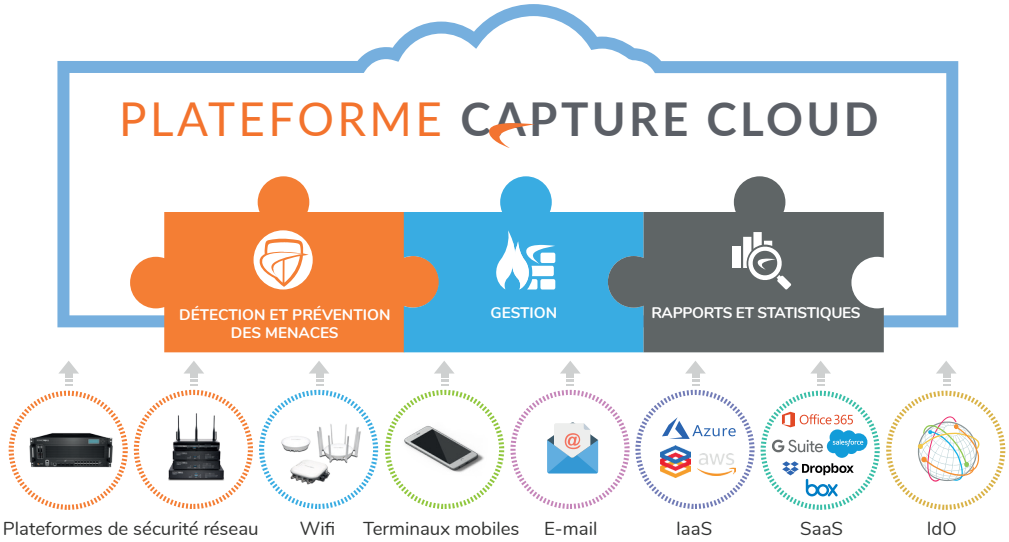
Sécurité SaaS basée sur les API fournissant des fonctionnalités CASB



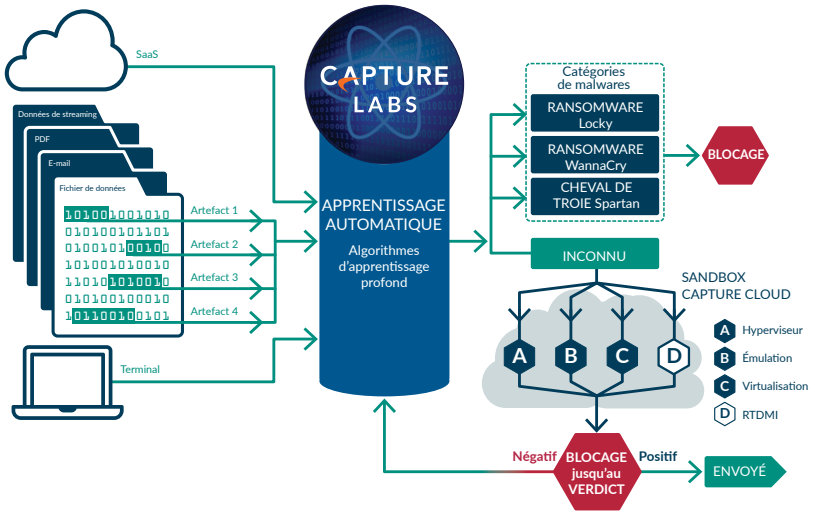
Le tableau de bord en temps réel permet aux administrateurs de surveiller l'utilisation des applications risquées, ainsi que de suivre l'activité des utilisateurs, le volume des transactions et la localisation depuis laquelle l'application est utilisée. La solution garantit une adoption sécurisée des applications SaaS sans impact sur la productivité des employés.

Intégration avec la plateforme Capture Cloud de SonicWall

La solution SonicWall Cloud App Security est un service de sécurité natif dans le cloud dont l'architecture repose sur la plateforme Capture Cloud et qui est fourni par Capture Security Center. La plateforme Capture Cloud de SonicWall assure la prévention des menaces et la gestion du réseau dans le cloud, à quoi s'ajoutent des fonctionnalités de reporting et d'analyse pour les entreprises de toute taille. Cette plateforme consolide les renseignements sur les menaces à partir de plusieurs sources dont notre service de sandboxing réseau multi-moteur primé, Capture Advanced Threat Protection, ainsi que plus de 1 million de capteurs SonicWall répartis dans le monde entier. Capture Security Center fournit une gestion sur écran unique et les administrateurs peuvent facilement créer à la fois des rapports des événements passés et en temps réel sur l'activité du réseau et du cloud.



Pour protéger les applications SaaS, SonicWall Cloud App Security exploite la plateforme SonicWall Capture Cloud, qui associe les renseignements globaux sur la sécurité du réseau Capture Threat Network avec la prévention avancée contre les menaces de la technologie sandbox multimoteur Capture ATP. Cette approche permet à SonicWall d'étendre ses capacités de prévention des intrusions automatisée en temps réel dans les environnements SaaS, donnant les moyens aux organisations de migrer dans le cloud. Les API natives s'intègrent directement aux services dans le cloud permettant à la solution d'analyser les fichiers dans les applications, comme OneDrive ou Dropbox en utilisant le service Capture ATP avec la technologie d'inspection approfondie de la mémoire en temps réel (RTDMI™), empêchant les ransomwares et les attaques « zero-day » de pénétrer dans le réseau.



Sécurité complète pour Office 365 et G Suite

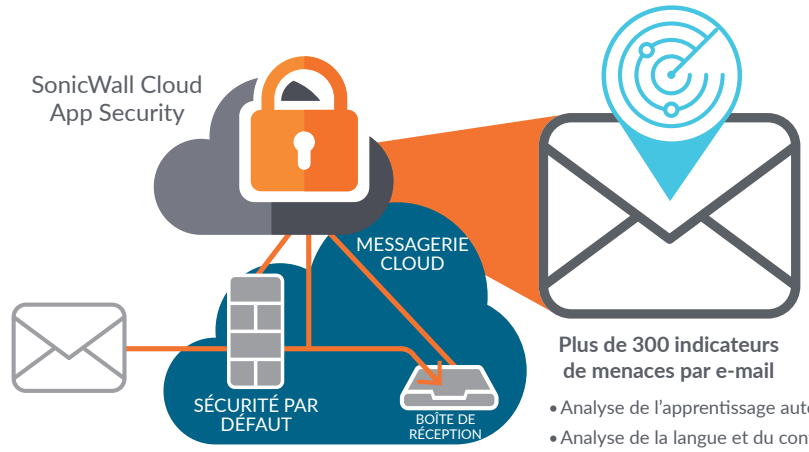
Une sécurité de nouvelle génération pour la messagerie électronique dans le Cloud

La solution SonicWall Cloud App Security comprend une sécurité de la messagerie de nouvelle génération conçue pour les plateformes de messagerie dans le cloud. Généralement, lorsque les entreprises migrent leur messagerie électronique dans le cloud, soit elles s'appuient exclusivement sur la sécurité intégrée du prestataire de messagerie électronique, soit elles la complètent avec un serveur mandataire pour les messages entrants (MTA). Les passerelles de messagerie externes, cependant, peuvent ne pas être suffisantes pour détecter et bloquer des menaces d'aujourd'hui.

En plus des couches de sécurité traditionnelles des messageries électroniques des vérifications SPF, DKIM et DMARC, ainsi que du filtrage des URL en exploitant trois principales sources de données pour les listes noires des URL, l'architecture unique de la solution Cloud App Security fournit une protection qui est impossible pour une solution passerelle externe :

- Ajoute une couche de protection contre les menaces avancées : la solution Cloud App Security bloque les messages de phishing ayant réussi à passer malgré Office 365 et G Suite. La solution exploite l'apprentissage automatique, l'intelligence artificielle et l'analyse du Big Data pour fournir une capacité puissante anti phishing, une technologie sandbox des pièces jointes et une protection avancée des URL, ainsi qu'une protection contre l'usurpation de l'identité.
- Surveille les messages électroniques entrants, sortants et internes : l'intégration SaaS de la solution Cloud App Security peut scanner et mettre en quarantaine chaque e-mail avant qu'il n'atteigne la boîte de réception d'un utilisateur, qu'il provienne de l'extérieur de l'entreprise ou d'un compte interne compromis.
- Scanne l'historique des messages pour détecter d'éventuelles menaces : dès la première connexion, la solution Cloud App Security scanne l'historique des messages (même les comptes fermés) pour détecter d'éventuelles intrusions ou des comptes compromis.
- Suppression globale d'e-mails : des messages malveillants peuvent être modifiés ou supprimés à tout moment, qu'ils soient malveillants, qu'ils contiennent des informations confidentielles ou après qu'un employé a répondu à tous par inadvertance.

Comme la protection de la messagerie électronique de la solution Cloud App Security est appliquée avant la boîte de la réception, mais après les filtres Microsoft ou Google natifs (ainsi que n'importe quelle passerelle MTA externe pouvant être déployée), ses algorithmes d'apprentissage automatique sont adaptés de manière unique pour identifier les menaces qui ont pu être ratées. Cloud App Security est également capable d'intégrer les résultats des scans natifs dans ses propres algorithmes de détection.



- Intégration complète avec Office 365 ou G Suite
- Contrôle total de la boîte de courrier : entrant, sortant, interne

Plus de 300 indicateurs de menaces par e-mail

- Analyse de l'apprentissage automatique
- Analyse de la langue et du contenu
- Service de sandboxing Capture ATP
- Protection avancée des URL

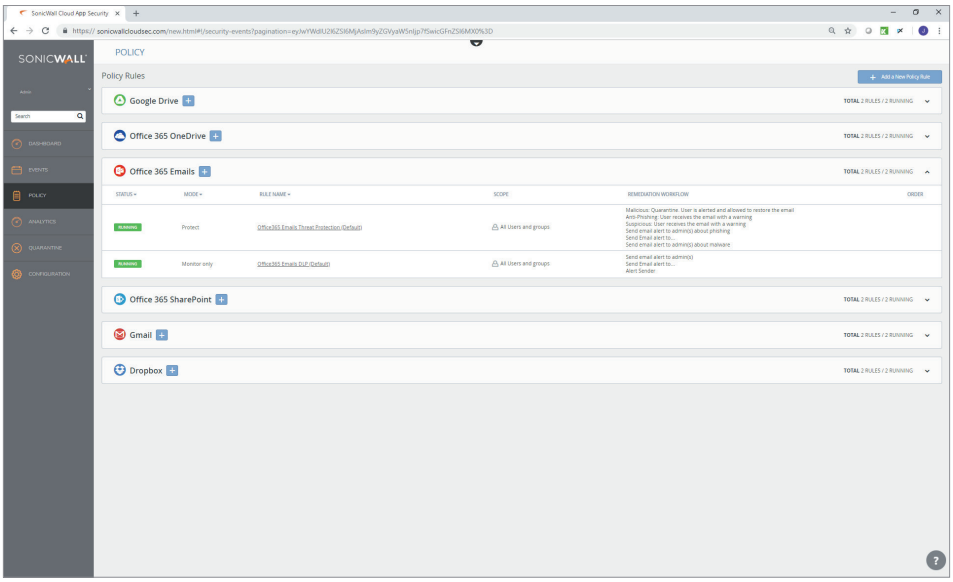
La protection conforme virtuelle bloque les messages malveillants avant qu'ils n'atteignent la boîte de réception des utilisateurs

Sécurité nouvelle génération pour la suite complète de productivité

Cloud App Security offre une sécurité complète de défense en profondeur pour Office 365 ou G Suite. Que vous utilisiez une messagerie électronique, des lecteurs partagés, des messageries instantanées ou l'environnement de pleine collaboration, la solution vous aide à :

- Éviter la propagation du phishing et des logiciels malveillants au sein de votre organisation ou jusqu'à vos clients et partenaires.
- Vérifier chaque fichier pour détecter un éventuel contenu malveillant en utilisant la technologie sandbox de Capture ATP et une analyse de contenu actif pour mettre en quarantaine les menaces avant qu'elles ne soient téléchargées par vos utilisateurs.
- Identifier les informations confidentielles et appliquer les règles compatibles au Cloud qui les contiennent au sein de l'organisation ou d'un groupe de travail. Vos utilisateurs peuvent exploiter tout le potentiel de la suite de productivité basée dans le cloud, tandis que les flux de travail automatisés garantissent la conformité réglementaire, s'assurant que les données PCI, HIPAA, DCP ou les autres données confidentielles ne sont pas partagées en externe.

Protection exhaustive pour la suite bureautique complète dans le cloud



Chaque application SaaS a un moteur de règles complètement différent, chacun avec ses propres règles et ses capacités d'application. Les solutions de SonicWall les cartographient sur les différentes applications SaaS autorisées et fournissent plus de contrôles granulaires. Ainsi, la solution Cloud App Security vous permet de créer une règle unique qui est appliquée d'une manière cohérente sur toutes les applications.

De plus, les règles contextuelles permettent de créer des flux de travail d'application qui informent l'utilisateur du problème, proposent des options sûres en termes de règles et auditent les réponses bien au-delà de ce que les contrôles d'autorisation intégrés dans chaque SaaS autorisent habituellement.

Sécurité SaaS

Pour sécuriser l'utilisation SaaS au sein des organisations, la solution SonicWall Cloud App Security fournit :

Une sécurité informatique autorisée : s'intègre directement aux services dans le cloud, à l'aide d'API pour une protection avancée contre les menaces et une prévention contre la fuite de données dans des environnements SaaS.

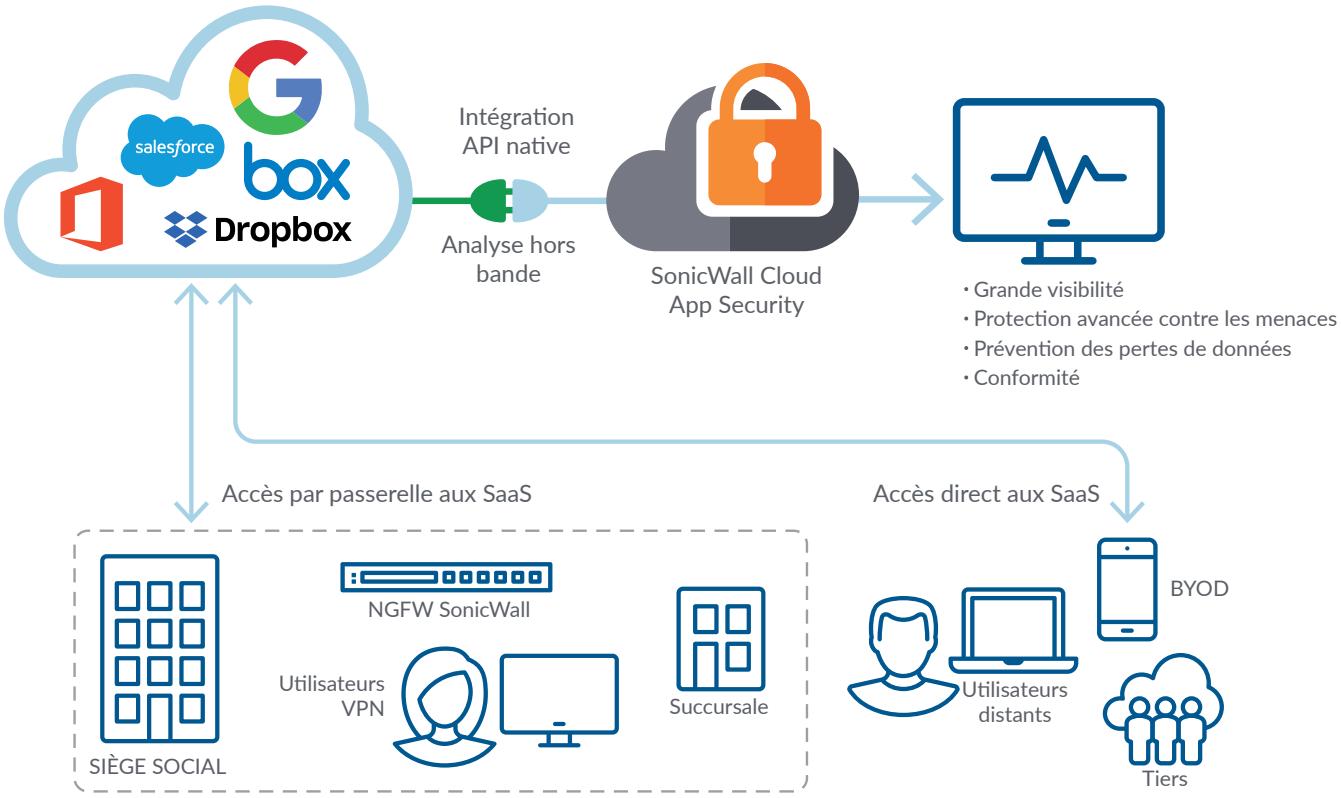
Visibilité et contrôle du « shadow IT » : intégration fluide avec les pare-feu de nouvelle génération SonicWall pour une découverte des applications automatisée dans le cloud et une évaluation des risques à l'aide de l'analyse des fichiers journaux du trafic.

Sécurité informatique autorisée

Lors de l'adoption d'applications SaaS comme Box et Dropbox, la responsabilité de garantir la sécurité des données incombe toujours à l'organisation et non au fournisseur de services cloud. Ces informations sont souvent divulguées dans les petits caractères et les fournisseurs de services cloud ne peuvent pas être tenus responsables d'une fuite de données ou d'une infection et d'une propagation de logiciels malveillants. Lorsque les organisations décident d'utiliser ces applications, elles doivent donc envisager de déployer une solution qui peut inspecter les données dans les applications cloud.

Seules les solutions basées sur des API peuvent inspecter les données inexploitées au sein des applications SaaS car les solutions conformes basées sur des proxys inspectent uniquement les données téléchargées sur le cloud depuis un emplacement protégé par un pare-feu. Comme de nombreuses entreprises ont déjà un gros volume de données stockées dans le cloud, les API sont utilisées pour appliquer des politiques sur ces données. D'autres fonctionnalités, uniquement possibles lors de la connexion directe à une application via une API, incluent la possibilité de scanner les paramètres de configuration de sécurité au sein de l'application et de suggérer des changements renforçant la sécurité, ainsi que la possibilité de scanner les autorisations de partage sur des fichiers et dossiers afin d'évaluer le risque que des tiers et des personnes externes accèdent à des données d'entreprise. La solution fournit une grande visibilité, une protection avancée contre les menaces à l'aide de la technologie sandbox Capture ATP et de la prévention des fuites de données pour les applications SaaS, comme les messageries électroniques dans le cloud, ainsi que les applications de partage de fichiers et de stockage dans le cloud, comme Google G Suite et Microsoft Office 365.

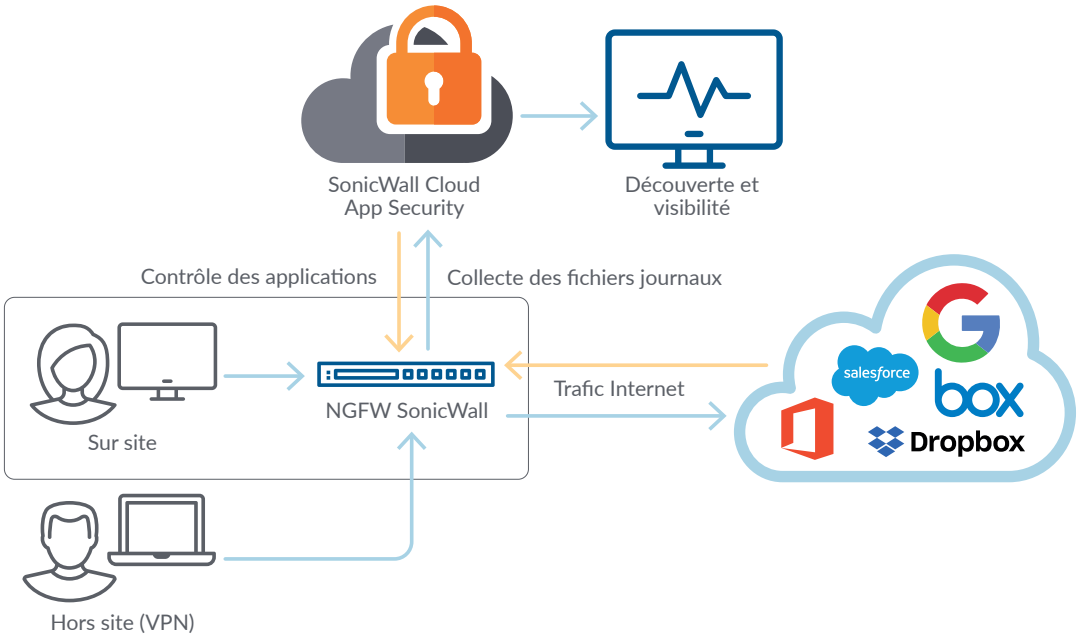
La solution SonicWall Cloud App Security analyse tout le trafic (par ex., événements des journaux de bord, activités des utilisateurs, fichiers et objets de données, état de configuration, etc.) et applique les politiques de sécurité nécessaires via des intégrations directes avec des API natives du service dans le Cloud. Comme la solution exploite les API natives, la solution n'utilise pas de proxy et ne se trouve pas entre l'utilisateur et le Cloud. Cela permet à la solution de fournir une protection pour les applications autorisées, quel que soit le dispositif ou le réseau de l'utilisateur. De plus, l'approche basée sur les API permet un déploiement facile et un contrôle granulaire, sans aucun impact sur l'expérience utilisateur.



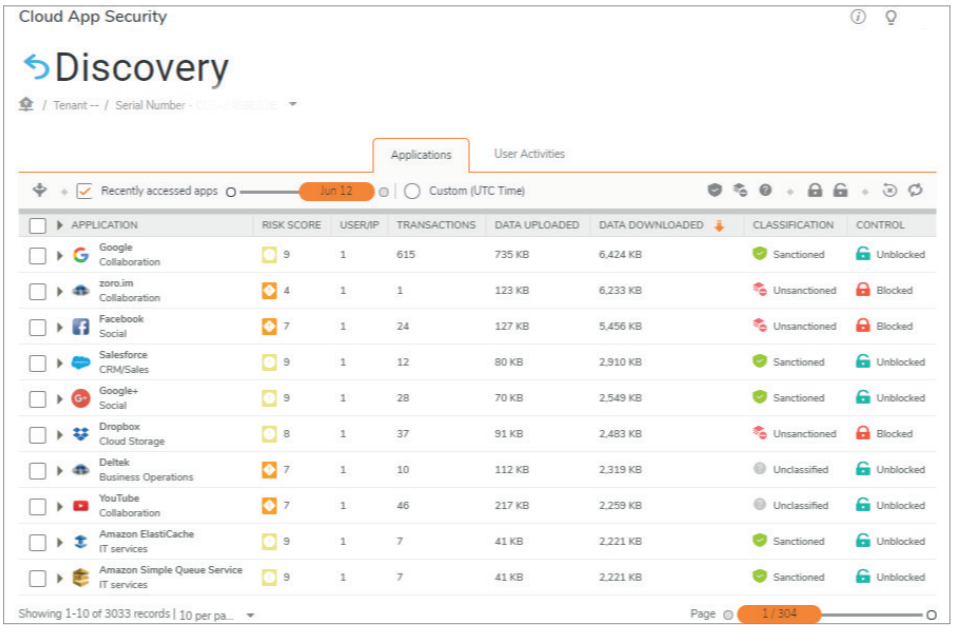
Applications SaaS autorisées sécurisées

Visibilité et contrôle du « shadow IT »

Les pare-feu de nouvelle génération SonicWall analysent et consignent l'ensemble du trafic qui entre et sort du réseau. Les journaux générés pour les données du trafic sortant ne distinguent pas clairement les applications Cloud utilisées et ne proposent pas de score de risque pour chaque application utilisée par les employés. Pour les employés nomades redirigés via un pare-feu de nouvelle génération avec VPN, la solution recueille à partir de ces journaux des détails supplémentaires sur les mesures que prennent les utilisateurs dans les services Cloud. Cloud App Security traite les fichiers journaux des pare-feu de nouvelle génération SonicWall et révèle les services Cloud en cours d'utilisation, identifient leurs utilisateurs, les volumes de données téléchargées depuis et vers le Cloud ainsi que le risque et la catégorie de chaque service Cloud. Avec Cloud App Security, l'infrastructure existante devient compatible Cloud. Tandis que les employés utilisent de plus en plus les applications Cloud dans un cadre professionnel, Cloud App Security permet aux administrateurs de détecter les lacunes dans la stratégie de sécurité, de classer les applications Cloud dans les catégories autorisées/interdites et d'appliquer des règles d'accès pour bloquer les applications à risque. Cloud App Security constitue une part essentielle de la vision de SonicWall consistant à fournir des capacités de détection et de prévention automatisées en temps réel des intrusions pour les clients lorsqu'ils adoptent les technologies dans le Cloud.



Découvrir le « shadow IT » dans votre réseau



La solution SonicWall Cloud App Security découvre et établit des rapports sur les services risqués du « shadow IT » en utilisant une base de données de réputation exclusive pour les services dans le cloud, gérée par SonicWall.

Les applications découvertes se voient attribuer un score de risque dérivé d'un algorithme reposant sur la réputation et sur des certifications de sécurité et de conformité. Les administrateurs informatiques peuvent classer des applications en se basant sur le score de risque comme étant des applications informatiques autorisées ou interdites d'utilisation. Via Capture Security Center, la solution permet aux administrateurs de configurer des règles de blocage/déblocage et de contrôler les activités du « shadow IT » sur le réseau.

Fonctionnalités

FONCTIONNALITÉ		AVANTAGE
Visibilité	Découverte des applications cloud	Automatise la découverte des applications cloud en exploitant les fichiers journaux de vos pare-feu SonicWall afin d'identifier les activités du « shadow IT » sur le réseau
	Visibilité de l'utilisation du cloud	Permet d'obtenir une représentation visuelle en temps réel des applications utilisées, du volume du trafic, de l'activité des utilisateurs et de la localisation de l'utilisation
	Évaluation des risques des applications	Prend des décisions éclairées pour bloquer/débloquer des applications en se basant sur l'évaluation des risques
	Surveillance des événements	Surveille chaque action, y compris les événements en temps réel et passés, prise dans votre environnement SaaS
Sécurité de la messagerie électronique de nouvelle génération	Anti-phishing	Bloque les attaques par phishing ciblées qui sont conçues pour échapper à la sécurité par défaut proposée par Office 365 ou G Suite
	Anti-spoofing	Protège votre marque d'entreprise et vos utilisateurs contre les e-mails frauduleux et les attaques par usurpation d'identités
	Technologie sandbox des pièces jointes	Bloque les pièces jointes d'e-mails malveillants avant qu'elles n'atteignent la boîte de réception de vos utilisateurs
	Protection avancée des URL	S'assure que les utilisateurs sont protégés contre les URL intégrées malveillantes
Protection avancée contre les menaces	Protection contre les logiciels malveillants de type « zero-day »	Empêche les logiciels malveillants d'être stockés et propagés via des applications comme Box, Dropbox, OneDrive et G Drive
	Protection contre le piratage des comptes	Protège les identifiants de connexion des SaaS en détectant tout comportement anormal des utilisateurs, d'éventuelles infractions aux autorisations ou modifications de configuration
Sécurité des données	Classification des données	Identifie les données sensibles ou confidentielles et applique les règles sur toutes les applications SaaS pour contrôler la façon dont ces informations peuvent être partagées.
	Contrôle d'accès centré sur les données	Gère les autorisations de fichiers en se basant sur le rôle de l'utilisateur et le type de données que le fichier contient
	Flux de travail de correction	S'assure que la sécurisation des données n'affecte pas les activités commerciales via une application en temps réel
Conformité	Modèles de conformité	Réduit les frais administratifs en utilisant des modèles de conformité simples pour répondre aux exigences des directives SOX, PCI, HIPAA et RGPD
	Piste d'audit	Accède aux données des événements passés pour l'audit de conformité rétrospectif, ainsi que pour l'établissement des rapports en temps réel
	Application des règles	Applique la conformité en temps réel avec chaque SaaS pour contrôler les autorisations d'accès, déplacer des fichiers, bloquer et modifier des e-mails et communiquer avec les utilisateurs et les administrateurs

SonicWall Cloud App Security	CLOUD APP SECURITY - BASIQUE	CLOUD APP SECURITY - AVANCÉE
Gestion unifiée du cloud (Capture Security Center)	●	●
Applications dans le cloud prises en charge	Sélectionner 1 application SaaS (Office 365 ou G Suite)	Choisir jusqu'à 10 applications SaaS
Anti-phishing pour O365 Mail ou Gmail	●	●
Capture ATP* pour les pièces jointes d'e-mails	●	●
Protection avancée des URL	●	●
Capture ATP* pour les fichiers stockés dans SaaS	●	●
Protection contre le piratage des comptes	●	●
Protection contre les pertes de données	—	●
Visibilité du « shadow IT »**	—	●

SonicWall Capture ATP comprend l'inspection approfondie de la mémoire en temps réel (Real-Time Deep Memory Inspection™, RTDMI™)
***Nécessite les NGFW SonicWall*

Informations de commande de Cloud App Security :

Pour obtenir plus d'informations sur la méthode de commande de Cloud App Security et la tarification, contactez votre partenaire ou l'équipe commerciale de SonicWall ici.

Cliquez ici (page en anglais) pour bénéficier d'un essai gratuit de 30 jours de la solution SonicWall Cloud App Security – Avancée

Pour plus d'informations sur Cloud App Security, visitez www.sonicwall.com/casb.

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.

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 - États-Unis
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Datasheet-CloudAppSecurity-US-VG-MKTG5359