SONICWALL CAPTURE SECURITY CENTER

Gestion Cloud unifiée dans un écran unique, analyse pour la sécurité des réseaux, des terminaux et du Cloud

SonicWall Capture Security Center est un logiciel de gestion de la sécurité dans le cloud, ouvert, évolutif et proposé en tant que service économique pour les entreprises et fournisseurs de services de différentes tailles et pour différents cas d'utilisation. C'est une solution optimale en termes de visibilité, d'agilité et de capacité à gérer de manière centralisée l'ensemble de l'écosystème de sécurité SonicWall avec davantage de clarté, de précision et de rapidité, le tout via une interface Cloud accessible partout et avec tout appareil compatible Web. Cette architecture orientée cloud et services unifie et connecte les services de sécurité et les outils de gestion SonicWall afin de gagner en efficacité opérationnelle et en élasticité, tout en permettant de déployer une stratégie de cyberdéfense plus vaste.

Guidé par les processus métier et les exigences de niveau de service, le Capture Security Center aide les SOC (Security Operation Centers) à fournir la base nécessaire à une stratégie unifiée de gouvernance de la sécurité, de conformité et de gestion des risques. En établissant une approche holistique connectée en matière d'orchestration de la sécurité, Capture Security Center fédère les aspects opérationnels de la sécurité des réseaux, des terminaux et du Cloud, via un framework de gestion commun simplifié. Il simplifie et, dans de nombreux cas, automatise de nombreuses tâches, ce qui améliore la coordination de la sécurité et la prise de décision, tout en réduisant la complexité, le temps et les dépenses liés aux opérations de sécurité et à l'administration. Ces tâches sont par exemple le provisioning des pare-feux et terminaux, la configuration, la surveillance, le reporting, la correction, l'audit et l'analyse du trafic et des données, précieuse dans la détection et la réaction aux problèmes de sécurité avant qu'ils ne se manifestent.

Avantages :

- Gestion centralisée de votre environnement de sécurité SonicWall, depuis un écran unique
- Réduction des silos de sécurité via un écran unique
- Amélioration de l'efficacité professionnelle grâce à la gestion des règles automatisée sans erreur
- Configuration simplifiée et accélérée des pare-feux distants avec le déploiement sans intervention
- Rapports de conformité simplifiés pour PCI, HIPPA et SOX
- Identification des lacunes et des risques de sécurité via des analyses précises et détaillées
- Réaction rapide aux risques avec des informations prioritaires sur les menaces

Le Capture Security Center assure l'authentification unique (SSO) pour déployer les licences, provisionner et gérer tous vos services de sécurité des réseaux, terminaux et cloud, notamment les services de gestion des pare-feux, d'analyse, Capture Client et Cloud Application Security. Notre vision consiste à unifier tout l'éventail des produits de sécurité SonicWall en un seul outil de gestion orienté intégration et englobe les services de sécurité Web, sans fil, e-mail, mobiles et IoT.[1] La combinaison de ces services Cloud permet de fournir une cyberprotection stratégique à plusieurs niveaux, des renseignements sur les menaces, des possibilités d'analyse et de collaboration, ainsi que des tâches courantes et synchronisées de gestion, de reporting et d'analyse. Le service d'abonnement actif comprenant les mises à jour logicielles et le support, l'accès aux dernières innovations et améliorations est immédiat. Cela aide à gérer les risques de sécurité, respecter les obligations réglementaires et se protéger contre les toutes dernières vulnérabilités et menaces, de manière automatisée. Évolutif et flexible à l'infini, le Capture Security Center s'adapte instantanément aux changements en termes de capacités et d'activité.

Gestion des cyber risques

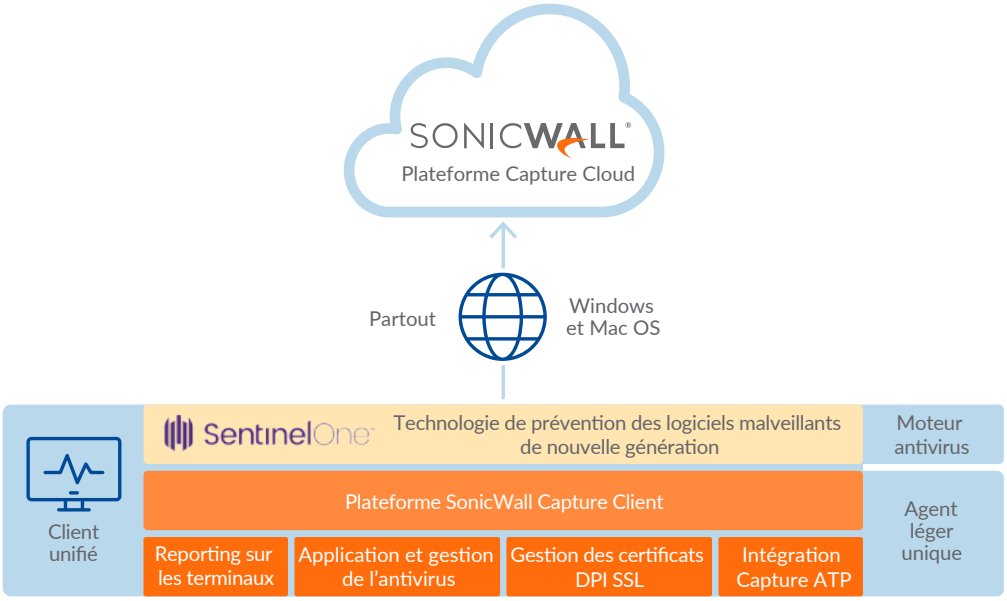
Intégré à la solution Capture Security Center, SonicWall Risk Meters est un outil puissant de gestion des informations de sécurité et des risques. Risk Meters fournit des données personnalisées sur les menaces et des scores de risque qui révèlent les lacunes dans les couches de défense, favorisent une planification décisive de la stratégie de sécurité et facilitent les actions nécessaires à une cyber défense optimale. Cela permet de renforcer la protection au niveau du réseau, du Cloud, du Web et des terminaux tout en réduisant la surface d'attaque visée par les menaces et la vulnérabilité de l'environnement face aux cyberattaques.

Par ailleurs, Risk Meters effectue une mise à jour continue du score de risque calculé et du niveau de menaces en fonction des données dynamiques sur les menaces et des capacités de défense existantes. Ces scores logiques peuvent alors permettre d'orienter la planification de la stratégie de sécurité ainsi que les décisions politiques et budgétaires.

Capture Client

Accessible au sein du Capture Security Center, SonicWall Capture Client est une plateforme client unifiée offrant de nombreuses fonctionnalités de protection des terminaux. Doté d'un moteur de protection anti-malware de nouvelle génération propulsé par SentinelOne, Capture Client applique des techniques de protection contre les menaces évoluées, comme l'apprentissage machine ou le rollback du système. Cela protège contre les logiciels malveillants agissant avec ou sans fichier, offre une vue à 360 degrés des attaques avec des informations exploitables, utiles pour mener l'enquête.

Associé aux pare-feux SonicWall, Capture Client assure une meilleure visibilité du trafic chiffré, via la gestion de certificats SSL de confiance utilisés pour l'inspection approfondie des paquets du trafic SSL/TLS.



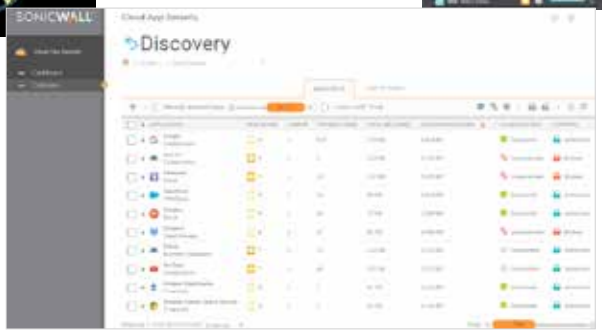
[1] *Les services de sécurité Web, sans fil, de messagerie, mobiles et IoT seront pleinement intégrés à cette plateforme lors de prochaines annonces sur le produit.*

Cloud App Security

L'abonnement au service d'analyse du SonicWall Capture Security Center procure aux clients une bonne visibilité sur le phénomène de Shadow IT et leur permet de contrôler l'utilisation des applications cloud. SonicWall Cloud App Security propose une fonctionnalité de type CASB. Elle permet aux administrateurs de déceler l'utilisation d'applications dangereuses, de suivre l'activité des utilisateurs et de définir des règles d'autorisation/blocage pour des applications, interdites ou non, sur les pare-feux gérés pour protéger les données sensibles.

Détection du Shadow IT, visibilité en temps réel, classification et contrôle des applications : telles sont les fonctionnalités clés du service Cloud App Security. Un service qui garantit un usage sécurisé des applications SaaS, sans entraver la productivité des employés et à un faible coût total de possession.

1. **Détection du Shadow IT :** s'appuie sur les fichiers journaux existants des pare-feux pour automatiser la fonction de découverte dans le cloud, en vue d'identifier les applications utilisées et leur niveau de risque.
2. **Visibilité des applications en temps réel :** surveille l'utilisation en temps réel grâce à un affichage intuitif sur tableau de bord, qui fournit des détails sur les applications utilisées, le volume du trafic, l'activité des utilisateurs et le lieu d'utilisation.
3. **Classification et contrôle des applications :** classifie les applications cloud non gérées selon les catégories « Sanctioned App » (approuvée par le service informatique) ou « Un-Sanctioned App » (non approuvée), et définit des règles d'autorisation/blocage en fonction du niveau de risque de l'application.



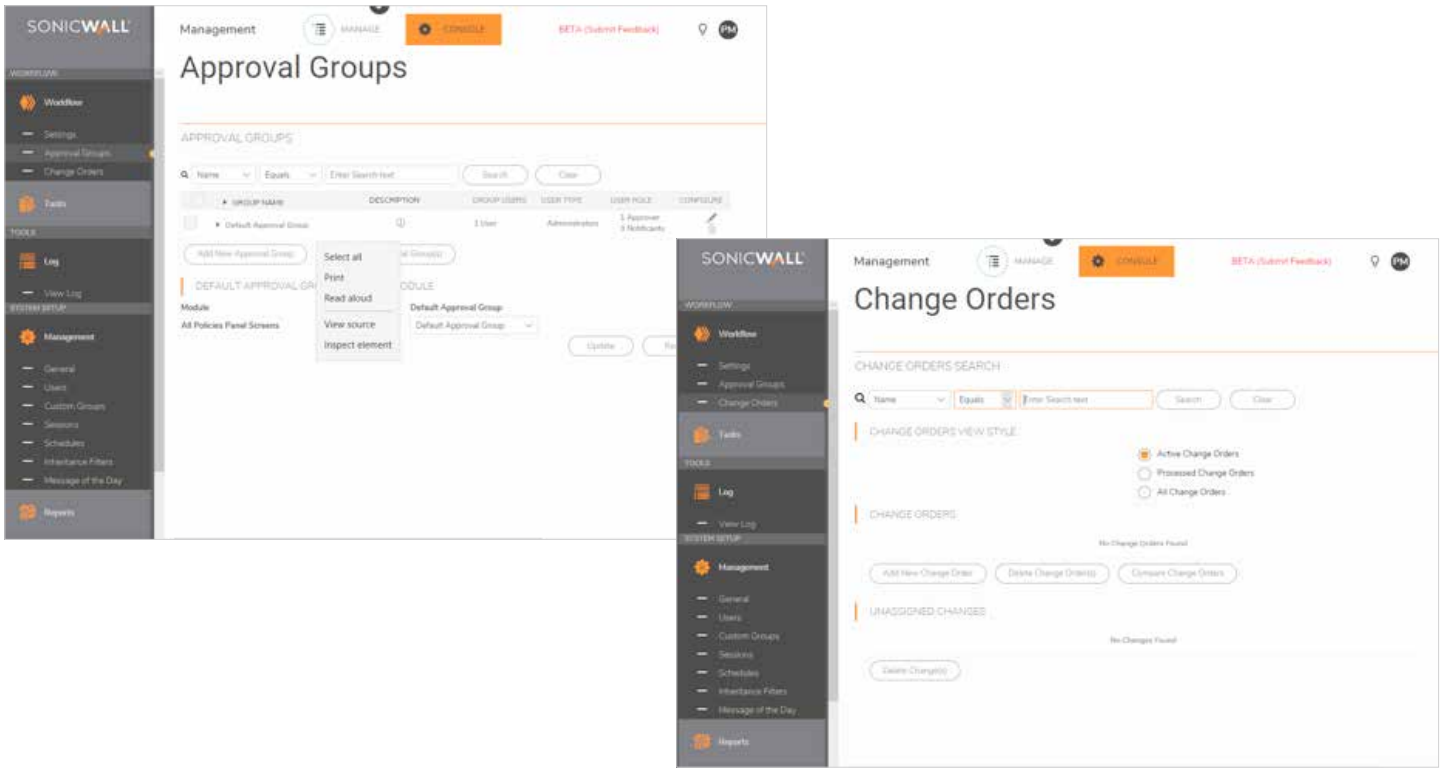
SONICWALL®

Automatisation du workflow

Grâce à l'automatisation native du workflow, le Capture Security Center permet aux SOC de se conformer à la gestion des modifications des règles de pare-feu et aux exigences en matière d'audit de diverses réglementations, telles que PCI, HIPAA et le RGPD. La modification des règles est rendue possible par une série de procédures rigoureuses de configuration, comparaison, validation, vérification et approbation des règles de pare-feu avant tout déploiement. Les groupes d'approbation sont flexibles, ce qui permet de se conformer aux diverses procédures d'autorisation et d'audit des différents types d'entreprises. L'automatisation du workflow programme le déploiement des règles de sécurité sanctionnées afin d'améliorer l'efficacité opérationnelle, de réduire les risques et d'éliminer les erreurs.

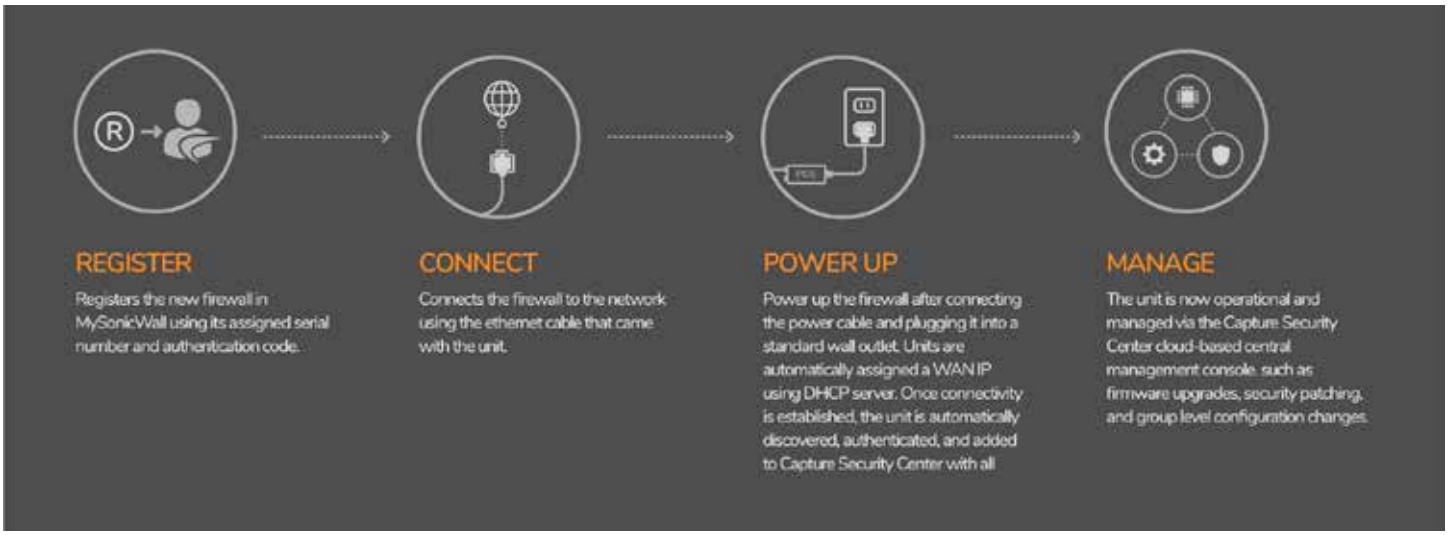
Le Capture Security Center fournit une approche globale en matière de gouvernance de la sécurité, de mise en conformité et de gestion des risques.

Automatisation du workflow : Cinq étapes pour une gestion des règles sans erreur



Déploiement zéro intervention

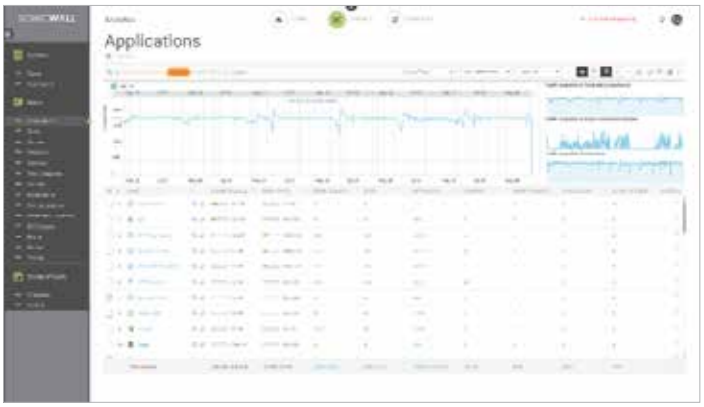
Intégré au Capture Security Center, le service de déploiement zéro intervention simplifie et accélère le processus de provisioning des pare-feux SonicWall dans les bureaux distants et les succursales. Ce processus ne demande qu'un minimum d'intervention de la part des utilisateurs et est entièrement automatisé de manière à rendre les pare-feux opérationnels à grande échelle en quatre étapes de déploiement simples. D'où une réduction significative du temps, des coûts et de la complexité liés à l'installation et la configuration, tandis que la sécurité et la connectivité sont assurées instantanément et automatiquement.

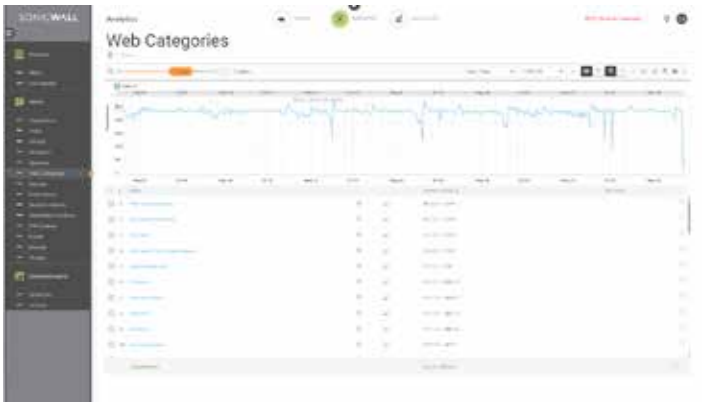


Déploiement zéro intervention : Rendez votre pare-feu opérationnel en quatre étapes simples

Reporting

Capture Security Center propose plus de 140 rapports prédéfinis et offre la possibilité de créer des rapports personnalisés en combinant des données vérifiables dans le but d'obtenir plusieurs résultats de cas d'utilisation. Ceux-ci intègrent une vision générale et détaillée des événements du réseau, des activités des utilisateurs, des menaces, des problèmes de fonctionnement et de performances, de l'efficacité de la sécurité, des risques et des failles de sécurité, de la préparation à la conformité, et même de l'analyse post-mortem. Chaque rapport est élaboré grâce à la contribution collective des clients et partenaires SonicWall. Cette longue collaboration permet d'obtenir une granularité, une portée et une connaissance approfondies des données syslog et IPFIX/NetFlow nécessaires pour suivre, mesurer et exécuter efficacement des opérations de réseau et de sécurité.

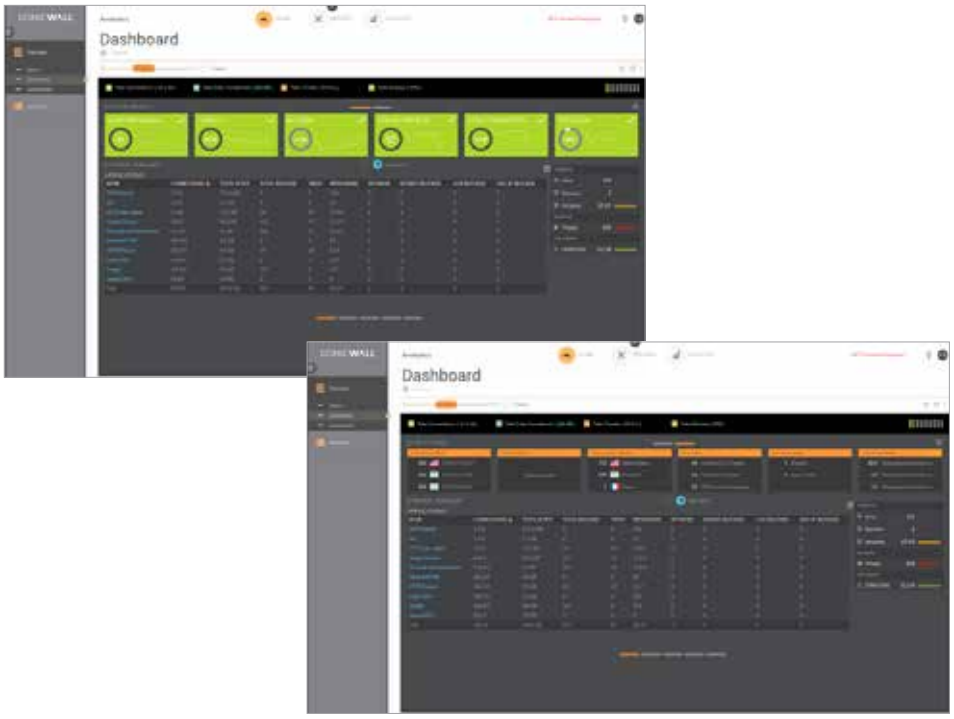


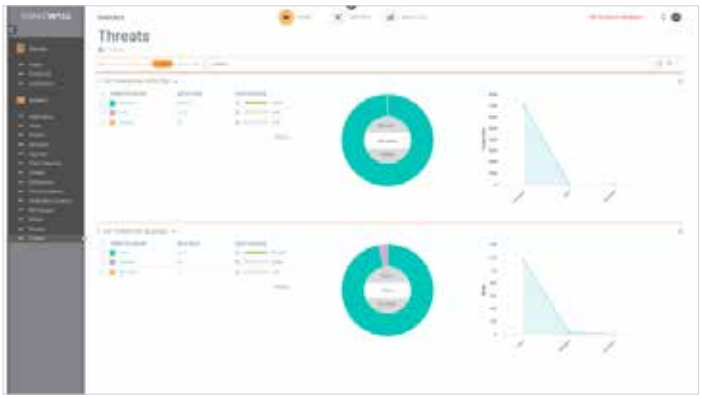


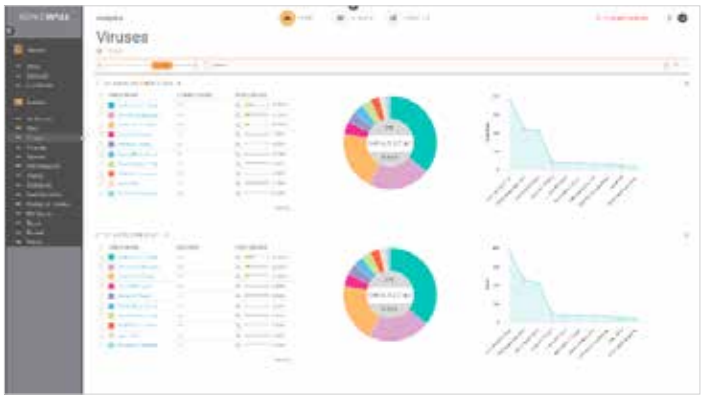
Analyse

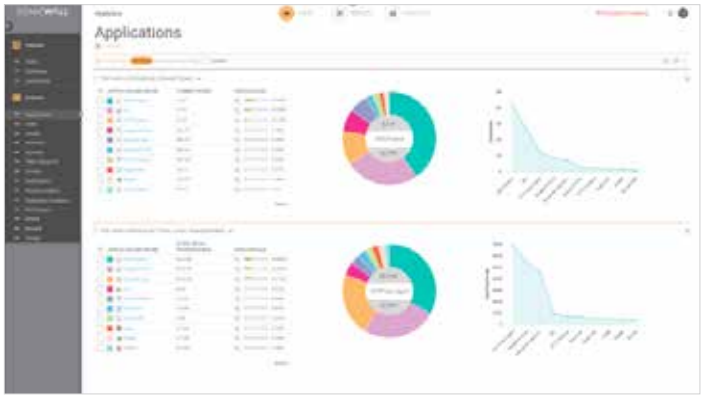
SonicWall Analytics est un moteur d'analyse décisionnelle big data qui automatise l'agrégation, la normalisation, la corrélation et la contextualisation des données de sécurité passant par tous les pare-feux gérés. Les organisations disposent ainsi d'une visibilité en temps réel sur tout ce qui se passe sur leur réseau. Les résultats, présentés de manière structurée, pertinente, exploitable et facilement consommable, permettent aux équipes de sécurité, analystes, auditeurs, conseils, dirigeants et autres parties prenantes de découvrir, d'interpréter et de prioriser les informations, de prendre des décisions et de mettre en œuvre les mesures défensives et correctives adaptées.

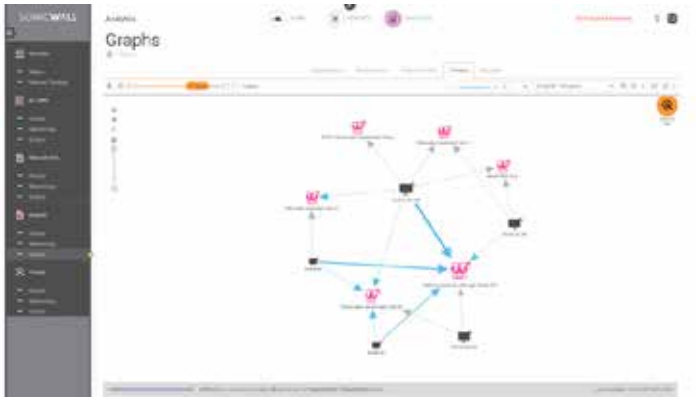
SonicWall Analytics offre une visualisation en temps réel, ainsi que des fonctionnalités de surveillance et d'alerte de données de sécurité enrichies, le tout sur un seul et même écran. Ce service fournit de puissants outils qui donnent aux clients toute l'autorité, l'agilité et la flexibilité nécessaires à la réalisation d'analyses approfondies avec zoom pour investigation du trafic réseau, de l'activité des utilisateurs, des événements de sécurité, du profil des menaces, de l'utilisation des applications et d'une foule d'autres données contextuelles des pare-feux. Cette visibilité, connaissance et compréhension en profondeur de l'environnement de sécurité procure aux clients une vue d'ensemble précieuse et la possibilité non seulement de déceler les risques en matière de sécurité, mais aussi d'orchestrer les mesures de correction, tout en surveillant et suivant les résultats avec davantage de clarté et plus rapidement. SonicWall Analytics permet d'opérationnaliser l'analyse de la sécurité et de l'intégrer aux processus métier, afin de transformer les données en informations, les informations en connaissances et les connaissances en décisions permettant d'obtenir une automatisation totale de la sécurité.

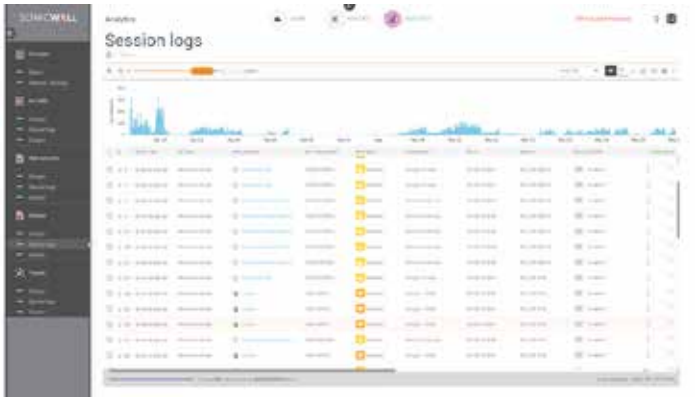










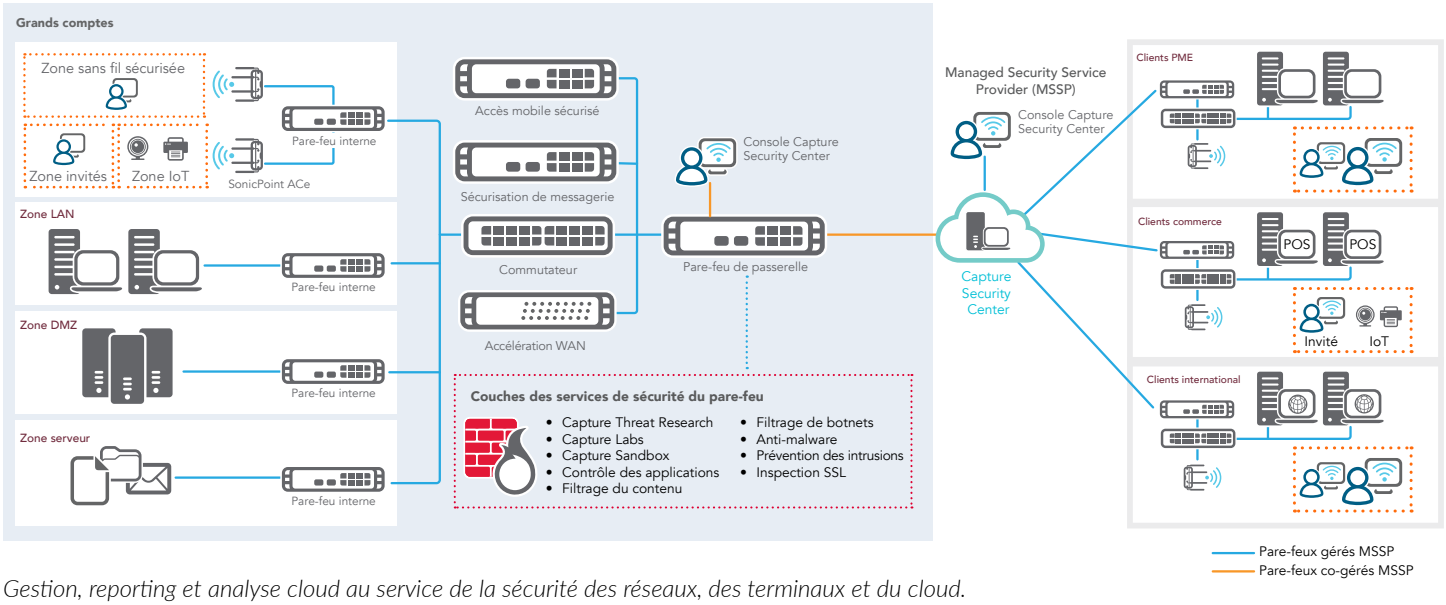


SONICWALL®

Architecture cloud évolutive

L'architecture distribuée du Capture Security Center favorise une disponibilité et une évolutivité du système à l'infini. Des petites aux grandes entreprises, en passant par les fournisseurs télécom, les opérateurs et fournisseurs de services présentant un écosystème fortement mutualisé, le Capture Security Center s'adapte à la demande et peut gérer des milliers de dispositifs de sécurité SonicWall, où qu'ils soient. Côté client, ses tableaux de bord universels hautement interactifs, chargés de données de surveillance, de reporting et d'analyse en temps réel, permettent de prendre des décisions éclairées et favorisent la collaboration, la communication et les connaissances sur toute la structure de sécurité partagée. Cette vue de l'environnement de sécurité à l'échelle de l'entreprise et une surveillance de la sécurité en temps réel qui atteint les bonnes personnes permettent d'établir des règles de sécurité précises et de prendre des mesures de contrôle avisées, pour une sécurité adaptative renforcée.

Le Capture Security Center constitue une plateforme de gestion, d'analyse et de reporting de la sécurité complète et évolutive pour les organisations distribuées et les fournisseurs de services (opérateurs, télécom ou fournisseurs de services gérés).



Gestion, reporting et analyse cloud au service de la sécurité des réseaux, des terminaux et du cloud.

Caractéristiques

Fonctionnalités de gestion de la sécurité et de surveillance	
Fonctionnalité	Description
Gestion centralisée de la sécurité et du réseau	Aide les administrateurs à déployer, gérer et surveiller un environnement de sécurité réseau distribué.
Configuration des règles fédérée	Permet de définir aisément des règles pour des milliers de pare-feux, points d'accès sans fil, commutateurs et équipements de sécurisation de messagerie et d'accès distant sécurisé, depuis un seul et même emplacement.
Gestion des ordres de modification et workflow	Assure exactitude et conformité des modifications des règles en appliquant un processus de configuration, comparaison, validation, révision et approbation des règles avant le déploiement. Les groupes d'approbation peuvent être personnalisés afin de respecter les règles de sécurité de l'entreprise. Toutes les modifications des règles sont consignées sous un format vérifiable qui garantit la conformité du pare-feu avec les contraintes règlementaires. Tous les détails des modifications effectuées sont conservés dans un historique afin de faciliter la mise en conformité, les pistes d'audit et le dépannage.
Déploiement zéro intervention	Simplifie et accélère le déploiement et le provisioning des pare-feux SonicWall à distance via le cloud. Envoie des règles, effectue les mises à jour du firmware et synchronise les licences automatiquement.
Configuration et déploiement VPN efficaces	Les commutateurs Dell série X peuvent désormais être facilement gérés au sein des pare-feux TZ, NS*a* et SuperMassive, offrant une gestion centralisée de toute l'infrastructure de sécurité du réseau.
Gestion hors ligne	Simplifie et accélère le déploiement et le provisioning des pare-feux SonicWall à distance via le cloud. Envoie des règles, effectue les mises à jour du firmware et synchronise les licences automatiquement.

Fonctionnalités de gestion de la sécurité et de surveillance (suite)	
Fonctionnalité	Description
Gestion rationalisée des licences	Simplifie l'activation de la connectivité VPN et consolide des milliers de règles de sécurité.
Tableau de bord universel	Réunit des widgets personnalisables, des cartes géographiques et des options de reporting relatives aux utilisateurs.
Système de surveillance active et d'alerte	Émet des alertes en temps réel avec options de surveillance intégrées, simplifie le dépannage en permettant aux administrateurs de prendre des mesures préventives et de remédier immédiatement aux problèmes.
Prise en charge SNMP	Fournit de puissants traps (interruptions) en temps réel pour l'ensemble des applications et dispositifs TCP/IP et SNMP, ce qui simplifie le dépannage et permet d'identifier les événements réseau critiques et d'y répondre.
Visualisation et contrôle des applications	Affiche des rapports historiques et temps réel indiquant quelles applications sont en cours d'utilisation et qui sont les utilisateurs. Les rapports sont entièrement personnalisables à l'aide de fonctionnalités intuitives de filtrage et de zoom.
Nombreuses options d'intégration	Fournit une interface de programmation applicative pour les services Web, la prise en charge CLI (interface en ligne de commande) pour la majorité des fonctions et la prise en charge de traps SNMP tant pour les fournisseurs de services que pour les entreprises.
Gestion des commutateurs réseau Dell série X	Les commutateurs Dell série X peuvent désormais être facilement gérés au sein des pare-feux TZ, NS*a* et SuperMassive, offrant une gestion centralisée de toute l'infrastructure de sécurité du réseau.
Risk Meters	Affiche les attaques dynamiques en temps réel, avec des graphiques détaillés qui enregistrent les activités malveillantes au niveau de la couche de défense spécifique. • Catégorisation des actions malveillantes des agresseurs au niveau de la couche de défense spécifique • Limite l'attention sur les attaques entrantes dans un environnement spécifique • Mise à jour du score de risque calculé et du niveau de menaces en fonction des données dynamiques sur les menaces et des capacités de défense existantes • Mise en évidence des lacunes de sécurité existantes permettant à des menaces évitables de profiter de l'insuffisance de protection • Mise en place d'actions de protection immédiates afin d'éviter toutes les menaces entrantes
Création de rapports	
Fonctionnalité	Description
Rapport sur les botnets	Il existe quatre types de rapports : Tentatives, Cibles, Initiateurs et Chronologie, contenant le contexte du vecteur de l'attaque, par ex. identifiant du botnet, adresses IP, pays, hôtes, ports, interfaces, initiateur/cible, source/destination et utilisateur.
Rapport Geo IP	Contient des informations sur le trafic bloqué en fonction de son pays d'origine ou de sa destination. Il existe quatre types de rapports : Tentatives, Cibles, Initiateurs et Chronologie, contenant le contexte du vecteur de l'attaque, par ex. identifiant du botnet, adresses IP, pays, hôtes, ports, interfaces, initiateur/cible, source/destination et utilisateur.
Rapport adresse Mac	Indique l'adresse MAC (Media Access Control) sur la page du rapport. Inclut des informations spécifiques à l'équipement (MAC Initiateur et MAC Répondant) dans cinq types de rapports : • Utilisation des données > Initiateurs • Utilisation des données > Répondants • Utilisation des données > Détails • Activité des utilisateurs > Détails • Activité Web > Initiateurs
Rapport Capture ATP	Affiche des informations détaillées sur le comportement de menaces, en réponse à une menace ou une infection.
Rapports HIPAA, PCI et SOX	Inclut des modèles prédéfinis de rapports PCI, HIPAA et SOX conformes aux exigences de sécurité des audits.

Création de rapports (suite)	
Fonctionnalité	Description
Rapports sur les points d'accès sans fil sauvages	Affiche tous les appareils sans fil en cours d'utilisation ainsi que le comportement sauvage lié à une mise en réseau ad-hoc ou poste à poste entre les hôtes et les associations accidentelles pour les utilisateurs qui se connectent aux réseaux sauvages voisins.
Rapports intelligents et visualisation des activités	Fournit des rapports graphiques et de gestion complets sur les pare-feux SonicWall, les équipements de sécurisation de messagerie et d'accès mobile sécurisé. Permet de mieux connaître les tendances d'utilisation et les événements de sécurité tout en fournissant une identité de marque cohérente pour les fournisseurs de services.
Journalisation centralisée	Offre un emplacement central pour consolider les événements de sécurité et les journaux de milliers d'appliances, ce qui permet de réaliser des analyses forensiques du réseau à partir d'un point unique.
Rapports syslog de nouvelle génération en temps réel et historiques	Simplifie, grâce à des améliorations révolutionnaires, le processus fastidieux de synthèse des données, permettant la génération en temps quasi réel de rapports sur les messages syslog entrants. Offre en outre la possibilité de zoomer sur les données ainsi que de nombreuses options de personnalisation des rapports.
Rapports universels planifiés	Planifie des rapports qui sont automatiquement créés et envoyés vers les destinataires autorisés pour plusieurs appliances de divers types.
Analyse	
Fonctionnalité	Description
Agrégation des données	Le moteur d'analyse décisionnelle automatise l'agrégation, la normalisation, la corrélation et la contextualisation des données de sécurité passant par tous les pare-feux.
Contextualisation des données	Des analyses exploitables, présentées de manière structurée, pertinente et facilement consommable, permettent aux équipes de sécurité, analystes et autres parties prenantes de découvrir, d'interpréter et de prioriser les informations, de prendre des décisions et de mettre en œuvre les mesures défensives adaptées.
Analyses de flux	Les flux de données de sécurité du réseau sont traités, corrélés et analysés en continu et en temps réel, et les résultats sont illustrés dans un tableau de bord visuel, dynamique et interactif.
Analyses utilisateur	Des analyses approfondies des tendances d'activité des utilisateurs offrent une visibilité totale des habitudes d'utilisation, d'accès et de connexion sur l'ensemble du réseau.
Visualisation dynamique en temps réel	Sur un seul et même écran, l'équipe de sécurité peut réaliser des analyses approfondies avec zoom pour investigation et forensiques des données de sécurité avec davantage de précision, de clarté et de rapidité.
Rapidité de détection et d'élimination	Des fonctionnalités d'investigation poursuivent les activités dangereuses et gèrent rapidement les risques en vue de les éliminer.
Analyse et reporting sur les flux	Fournit un agent de création de rapports sur les flux pour l'analyse du trafic applicatif et sur les données d'utilisation via les protocoles IPFIX ou NetFlow, pour une surveillance en temps réel et historique. Offre aux administrateurs une interface efficace pour surveiller visuellement leur réseau en temps réel. Ils peuvent ainsi identifier les applications et sites Web très consommateurs en bande passante, voir l'utilisation que fait chaque utilisateur des applications et anticiper les attaques et menaces rencontrées sur le réseau. • Un visualiseur en temps réel avec personnalisation par glisser-déposer • Un écran de rapport en temps réel avec filtrage en un clic • Un tableau de bord des principaux flux avec boutons d'affichage en un clic • Un écran de rapport sur les flux avec cinq onglets d'attributs de flux supplémentaires • Un écran d'analyse des flux avec puissantes fonctionnalités de corrélation et de rotation • Un visualiseur de sessions pour les zooms avant détaillés de sessions et de paquets.
Analyse du trafic applicatif	Fournit des informations précieuses sur le trafic applicatif, la consommation de bande passante et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique.
Cloud App Security	
Fonctionnalité	Description
Tableau de bord en temps réel	Offre une représentation visuelle en temps réel des applications utilisées, du volume du trafic, de l'activité des utilisateurs et du lieu d'utilisation.
Détection des applications	La détection d'applications cloud peut être automatisée grâce aux fichiers journaux de votre pare-feu SonicWall, en vue d'identifier les activités de Shadow IT sur le réseau.
Évaluation du niveau de risque des applications	Permet de prendre des décisions éclairées concernant le blocage/déblocage d'applications en fonction de l'évaluation des risques.
Classification et contrôle des applications	Permet de classer les applications selon qu'elles sont approuvées ou non et de définir des règles de blocage des applications dangereuses.

Récapitulatif des fonctionnalités

Gestion

- Accès universel
- Alertes et notifications
- Outils de diagnostic
- Sessions utilisateur multiples et simultanées
- Gestion et planification hors ligne
- Gestion des règles de sécurité des pare-feux
- Gestion des règles de sécurité VPN
- Gestion des règles de sécurité de messagerie
- Gestion des règles d'accès distant sécurisé/VPN SSL
- Gestion des services de sécurité à valeur ajoutée
- Définition des modèles de règles au niveau groupe
- Réplication des règles appareil vers groupe d'appareils
- Réplication des règles niveau groupe vers appareil unique
- Redondance et haute disponibilité
- Gestion du provisioning
- Architecture évolutive et distribuée
- Vues dynamiques de gestion
- Gestionnaire de licences unifié
- Interface de ligne de commande
- Interface de programmation applicative (API) de services Web
- Gestion basée sur les rôles (utilisateurs, groupes)
- Tableau de bord universel
- Sauvegarde des fichiers de préférences pour les pare-feux

Surveillance

- Flux de données IPFIX en temps réel
- Prise en charge SNMP
- Système de surveillance active et d'alerte
- Gestion des relais SNMP
- Surveillance de l'état des VPN et pare-feux
- Surveillance Syslog dynamique et alertes
- Risk Meters

Création de rapports

- Éventail complet de rapports graphiques
- Rapports de conformité
- Rapports personnalisables avec fonctionnalités de zoom
- Journalisation centralisée
- Rapports multi-menaces
- Rapports axés sur les utilisateurs
- Rapports d'utilisation des applications
- Rapports granulaires de services
- Fonctions intelligentes d'analyse des attaques
- Bande passante et rapport de services par interface
- Rapports pour pare-feux UTM SonicWall
- Rapports pour appliances SRA SSL VPN SonicWall
- Rapports universels planifiés
- Rapports Syslog et IPFIX de nouvelle génération
- Rapports flexibles et granulaires en temps quasi réel
- Rapports sur la bande passante par utilisateur
- Rapports sur l'activité Client VPN
- Résumé détaillé du rapport de services VPN
- Rapports sur les points d'accès sans fil sauvages
- Rapports WAF (Web Application Firewall) SRA pour PME
- Rapports Cloud App Security (CAS)
- Rapports Capture Client

Analyse

- Agrégation des données
- Contextualisation des données
- Analyses de flux
- Analyses utilisateur
- Visualisation dynamique en temps réel
- Rapidité de détection et d'élimination

Licences et packages

Les services Cloud CSC Management, Reporting, Analytics et CAS sont disponibles pour les options ci-dessous, avec une condition requise minimum : chaque pare-feu géré doit avoir un abonnement AGSS ou CGSS actif.

1. CSC Basic Management (Lite)

Cette version convient particulièrement à la sauvegarde/restauration de votre système pare-feu ou des préférences, ainsi que pour la mise à jour des firmware. Tout pare-feu avec abonnement AGSS ou CGSS peut être équipé de cette fonctionnalité de gestion de base, activée pour aider à administrer les pare-feux.

2. CSC Management

Cette option d'abonnement payant active des fonctionnalités de gestion complètes, notamment Workflow Automation et Zero-Touch Deployment.

3. CSC Management and Reporting

Cette option de licence est idéale pour les grandes entreprises équipées de nombreux pare-feux dont le déploiement est géographiquement dispersé, et dont la gestion est exécutée au niveau groupe ou mutualisée. Il s'agit des PME, des entreprises distribuées, des entreprises du secteur public et des établissements d'enseignement composés de plusieurs groupes scolaires et campus, ainsi que des fournisseurs de services gérés (MSP).

Outre les fonctionnalités complètes de gestion, cette option d'abonnement fournit des fonctionnalités complètes de création de rapports permettant d'effectuer des examens et des audits réguliers ou à la demande sur la sécurité et les performances du réseau. Cela peut être effectué via l'écran interactif du tableau de bord universel, avec graphiques et tableaux, ou hors écran avec des rapports planifiés et exportés.

4. CSC Analytics

Il s'agit d'un service complémentaire puissant disponible pour toutes les options d'abonnement à Capture Security Center. L'activation de ce service permet de bénéficier d'un accès total aux outils et services SonicWall Analytics et SonicWall Cloud App Security, en vue d'une analyse forensique réseau et d'une chasse aux menaces à l'aide de fonctionnalités complètes de zoom avant et de rotation.

	Caractéristiques	CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Gestion	Sauvegarde/Restauration – système pare-feu	Oui	Oui	Oui	Oui
	Sauvegarde/Restauration – préférences de pare-feu	Oui	Oui	Oui	Oui
	Mise à jour firmware	Depuis fichier local uniquement	Depuis fichier local uniquement ou MySonicWall	Oui	Depuis fichier local uniquement
	Planification des tâches	–	Oui	Oui	–
	Gestion de groupes de pare-feux	–	Oui	Oui	–
	Héritage – direct et inverse	–	Oui	Oui	–
	Déploiement sans intervention[1]	–	Oui	Oui	–
	Téléchargements de signatures des pare-feux hors ligne	–	Oui	Oui	–
	Workflow	–	Oui	Oui	–
	Licences groupées – Recherche, partage, inventaire des codes d'activation utilisés	–	Oui	Oui	–
Rapports (Netflow/ IPFIX)	Planification de rapports, Live Monitor, tableaux de bord récapitulatifs	–	–	Oui	Oui
	Rapports téléchargeables : applications, menaces, CFS, utilisateurs, trafic, source/destination (rapports sur les flux, 1 an)	–	–	Oui	Oui
Analyse (Netflow/IPFIX)	Analyse forensique réseau et chasse aux menaces avec zooms avant et rotations	–	–	–	Oui
	Cloud App Security	–	–	–	Oui
	Conservation de données du trafic 30 jours	–	–	–	Oui
Support technique		Dossiers Web uniquement	Support 24X7	Support 24X7	Support 24X7

[1] *Pris en charge pour SOHO-W avec firmware 6.5.2+; TZ, NSA Series et NSa 2650-6650 avec firmware 6.5.1.1+. Non pris en charge pour SOHO ou NSv Series.*

Modèles de pare-feux pris en charge

Capture Security Center est disponible uniquement pour les clients AGSS/CGSS avec pare-feux SOHO-W, TZ Series, NSA Series, NS*a* 2650-6650 et NS*v* Series. Pour SuperMassive 9000, NS*a* 9250 à 9650 et NS*sp* 12400 à 12800, l'option d'abonnement à CSC Management est automatiquement activée sur activation de l'abonnement AGSS correspondant.

Capture Security Center			
	Gestion	Création de rapports	Analytics
Pare-feu entrée de gamme	SOHO-W, TZ Series, NS*v* 10-100	TZ Series, NS*v* 10-100	TZ Series, NS*v* 10-100
Pare-feu milieu de gamme	NSA Series, NS*a* 2650-6650, NS*v* 200-400	NSA Series, NS*a* 2650-6650, NS*v* 200-400	NSA Series, NS*a* 2650-6650, NS*v* 200-400
Pare-feu haut de gamme	SuperMassive 9000 Series, NS*sp* 12000 Series, NS*a* 9250-9650, NS*v* 800-1600		

Informations de commande

Produit	Référence
SonicWall Capture Security Center Management pour TZ Series, SOHO-W, NSv 10 à 100, 1 an	01-SSC-3664
SonicWall Capture Security Center Management pour TZ Series, SOHO-W, NSv 10 à 100, 2 ans	01-SSC-9151
SonicWall Capture Security Center Management pour TZ Series, SOHO-W, NSv 10 à 100, 3 ans	01-SSC-9152
SonicWall Capture Security Center Management pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 1 an	01-SSC-3665
SonicWall Capture Security Center Management pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 2 ans	01-SSC-9214
SonicWall Capture Security Center Management pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 3 ans	01-SSC-9215
SonicWall Capture Security Center Management and Reporting pour TZ Series, NSv 10 à 100, 1 an	01-SSC-3435
SonicWall Capture Security Center Management and Reporting pour TZ Series, NSv 10 à 100, 2 ans	01-SSC-9148
SonicWall Capture Security Center Management and Reporting pour TZ Series, NSv 10 à 100, 3 ans	01-SSC-9149
SonicWall Capture Security Center Management and Reporting pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 1 an	01-SSC-3879
SonicWall Capture Security Center Management and Reporting pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 2 ans	01-SSC-9154
SonicWall Capture Security Center Management and Reporting pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 3 ans	01-SSC-9202
SonicWall Capture Security Center Analytics pour TZ Series, NSv 10 à 100, 1 an	02-SSC-0171
SonicWall Capture Security Center Analytics pour NSA 2600 à 6600, NSa 2650 à 6650 et NSv 200 à 400, 1 an	02-SSC-0391

Navigateurs Internet

- Microsoft® Internet Explorer 11.0 ou version supérieure (ne pas utiliser le mode de compatibilité)
- Mozilla Firefox 37.0 ou version supérieure
- Google Chrome 42.0 ou version supérieure
- Safari (version la plus récente)

Appliances SonicWall prises en charge gérées par Capture Security Center

- Appliances de sécurité réseau SonicWall : NS*a* 2600 à NS*a* 6650 et TZ Series
- Appliances virtuelles de sécurité réseau SonicWall : NS*v* 10 à NS*v* 400
- Sécurité des terminaux SonicWall – Capture Client
- Sécurité cloud – SonicWall Cloud App Security (CAS)

À propos de nous

SonicWall s'engage depuis plus de 27 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 automatisée de détection et de prévention des failles en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 215 pays et territoires, leur permettant de se concentrer sans crainte sur leur cœur de métier. Pour plus d'informations, consultez notre site à l'adresse : **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-CaptureSecurityCenter-US-VG-MKTG4268