SonicWall Analytics

Transformer les données en informations, les informations en connaissances, les connaissances en décisions et les décisions en actions

SonicWall Analytics fournit une vue plongeante sur tout ce qui survient au sein de l'environnement de sécurité réseau SonicWall, le tout via un écran unique. En son cœur réside un puissant moteur d'analyse orienté décisionnel qui automatise l'agrégation, la normalisation, la corrélation et la contextualisation des données de sécurité qui transitent par tous les pare-feux et points d'accès sans fil SonicWall. Le tableau de bord interactif de l'application utilise divers formats de graphiques et de tableaux de budget-temps pour créer des représentations de connaissances des modèles de données.

Analytics présente les résultats de manière pertinente, actionnable et facilement consommable. Cela permet aux équipes de sécurité, aux analystes, aux auditeurs et aux équipes dirigeantes de découvrir, interpréter, définir des priorités, prendre des décisions sur la base de données factuelles ainsi que des mesures appropriées de protection et de correction contre les risques et les menaces qui apparaissent tout au long du processus de découverte.

Analytics fournit aux acteurs concernés des renseignements en temps réel ainsi qu'une visibilité, un contrôle et une flexibilité centralisés. Ils peuvent ainsi effectuer des analyses approfondies avec zoom avant pour investigation et forensique du trafic réseau, de l'accès utilisateur, de la connectivité, des applications et de l'utilisation, de l'état des ressources de sécurité, des événements de sécurité, des profils des menaces et autres données relatives aux pare-feux.

Avantages :

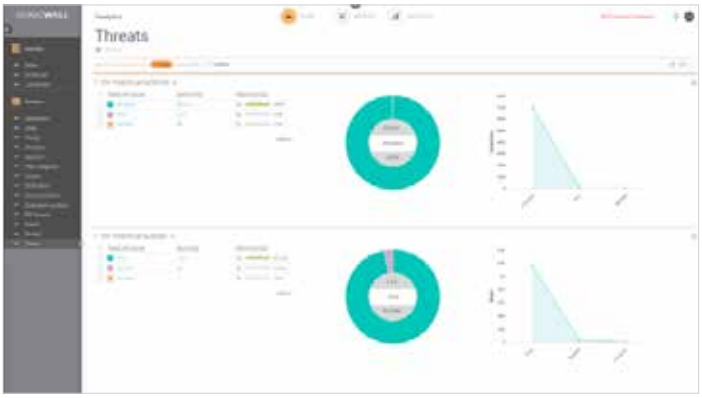
- Visibilité centralisée et identification complète en situation de l'environnement de sécurité réseau
- Autorité et flexibilité totales pour effectuer des analyses approfondies pour investigation et forensique
- Connaissances approfondies et compréhension des menaces et des risques réels et potentiels
- Corrections adaptées aux risques avec plus de clarté, de certitude et de rapidité
- Réduction du temps de réponse aux incidents grâce à des renseignements sur les menaces, en temps réel et actionnables

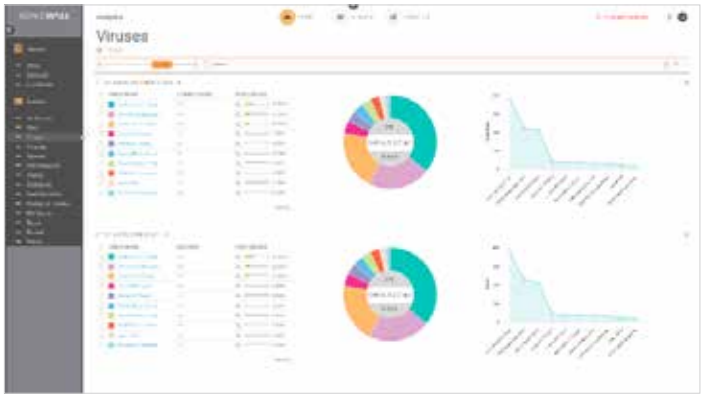
Partner Enabled Services

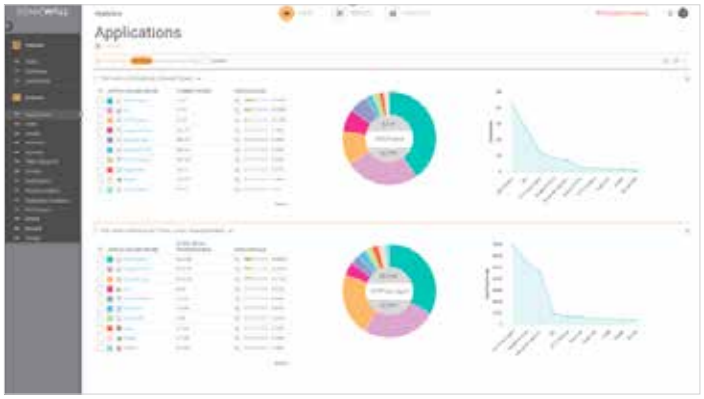
Vous avez besoin d'aide pour planifier, déployer et optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous offrir des services professionnels de premier ordre. Pour en savoir plus, rendez-vous sur www.sonicwall.com/PES.

Cette connaissance et cette compréhension approfondies de l'environnement de sécurité permet de disposer des renseignements et des capacités nécessaires pour identifier et orchestrer les mesures de correction adaptées aux risques de sécurité, ainsi que de surveiller et suivre les résultats avec davantage de clarté, de certitude et de rapidité.

L'intégration d'Analytics dans le processus métier permet d'opérationnaliser l'analyse et ainsi de transformer les données en informations, les informations en connaissances et les connaissances en décisions afin de parvenir à une automatisation de la sécurité.







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 sans intervention	Simplifie et accélère le déploiement et la configuration des pare-feux SonicWall avec utilisation du Cloud à distance. Déploie automatiquement les règles, effectue les mises à jour de firmware et synchronise les licences.
Configuration et déploiement VPN efficaces	Les commutateurs réseau Dell X Series peuvent désormais être facilement gérés au sein des pare-feux TZ, NSa et SuperMassive pour offrir une gestion centralisée sur l'ensemble de l'infrastructure de sécurité du réseau.
Gestion hors ligne	Simplifie et accélère le déploiement et la configuration des pare-feux SonicWall avec utilisation du Cloud à distance. Déploie automatiquement les règles, effectue les mises à jour de firmware et synchronise les licences.
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 avant.
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 X Series	Les commutateurs réseau Dell X Series peuvent désormais être facilement gérés au sein des pare-feux TZ, NSa et SuperMassive pour offrir une gestion centralisée sur l'ensemble de l'infrastructure de sécurité du réseau.
Rapports HIPPA, PCI et SOX	Inclut des modèles prédéfinis de rapports PCI, HIPAA et SOX conformes aux exigences de sécurité des audits.
Analytics	
Fonctionnalité	Description
Agrégation de données	Le moteur d'analyse orienté décisionnel automatise l'agrégation, la normalisation, la corrélation et la contextualisation des données de sécurité qui transitent par tous les pare-feux.
Contextualisation des données	Des analyses actionnables, présentées de manière structurée, pertinente et facilement consommable, permettent aux équipes de sécurité, analystes et acteurs concernés de découvrir, interpréter, définir des priorités, prendre des décisions et déterminer les mesures de protection appropriées.
Analyse de flux	Les flux de données de sécurité réseau sont traités, corrélés et analysés en continu et en temps réel et les résultats sont présentés dans un tableau de bord visuel dynamique et interactif.
Analyses utilisateurs	Analyse approfondie des tendances d'activité des utilisateurs afin d'obtenir une visibilité complète sur leur utilisation, leur accès et leurs connexions sur l'ensemble du réseau.
Visualisation dynamique en temps réel	Via un écran unique, l'équipe de sécurité peut effectuer des analyses approfondies avec zoom avant pour investigation et forensique sur les données de sécurité, avec davantage de clarté, de certitude et de rapidité.
Détection et correction rapides	Fonctionnalités d'investigation pour détecter les activités à risque et rapidement gérer les risques et y apporter des corrections adaptées.
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.

Récapitulatif des fonctionnalités

Tableau de bord récapitulatif avec visualisations et graphiques

- Débit de bande passante
- Utilisation du processeur
- Nombre de connexions
- Vitesse de connexion
- Indice de risque (échelle 1-10)
- Pourcentage de blocage
- Nombre total de connexions
- Volume total de données transférées
- Principales applications
- Principales intrusions
- Principales catégories URL
- Principaux virus
- Nombre de virus, intrusions, logiciels espions, botnets

Streaming Live Monitor avec graphiques en aires/à barres

- Applications
- Interface entrée/sortie, moyenne, min, max
  - Bande passante
  - Vitesse paquets
  - Taille paquets
  - Vitesse de connexion
- Utilisation
  - Nombre de connexions
  - Surveillance multiprocesseur

Principaux tableaux de bord récapitulatifs avec zooms avant

- Applications
- Utilisateurs
- Virus
- Intrusions
- Logiciels espions
- Catégories Web
- Sources
- Destinations
- Emplacements sources
- Emplacements destinations
- Files d'attente bande passante
- Botnet

Rapports avec zooms avant, exportation vers pdf/csv et e-mailing planifié

- Applications / Utilisateurs / Sources / Destinations
  - Connexions
  - Nombre total de connexions bloquées
  - Connexions bloquées par règle d'accès
  - Connexions bloquées par menace
  - Connexions bloquées par filtre botnet
  - Connexions bloquées par filtre GeoIP
  - Connexions bloquées par Content Filtering Service
  - Virus
  - Intrusions
  - Logiciels espions
  - Volume total de données transférées
  - Données envoyées
  - Données reçues
- Virus / Intrusions / Logiciels espions / Catégories Web / Emplacements sources / Emplacements destinations / Files d'attente bande passante
  - Connexions
  - Volume total de données transférées
  - Données envoyées
  - Données reçues
- Botnet
  - Connexions
- Export
  - .pdf
  - .csv
- Rapports planifiés
  - Rapports sur les flux
  - Capture Threat Assessment (SWARM)
  - Jour / Semaine / Mois
  - Archive / E-mail / PDF

Visualiseur de sessions Analytics avec zooms avant, filtrage, exportation de données de sessions individuelles

- Analyse du trafic pour toute combinaison de :
  - Application
  - Catégorie de l'application
  - Risque de l'application
  - Signature
  - Action
  - IP initiateur/répondant
  - Pays initiateur/répondant
  - Port initiateur/répondant
  - Octets initiateur/répondant
  - Interface initiateur/répondant
  - Index initiateur/répondant
  - Passerelle initiateur/répondant
  - MAC initiateur/répondant
  - Protocole
  - Vitesse (kbit/s)
  - ID flux
  - Intrusion
  - Virus
  - Logiciels espions
  - Botnet
- Menaces/analyses bloquées pour toute combinaison de :
  - Nom menace
  - Type menace
  - ID menace
  - Application
  - Catégorie de l'application
  - Risque de l'application
  - Signature
  - Action
  - IP initiateur/répondant
  - Pays initiateur/répondant
  - Port initiateur/répondant
  - Octets initiateur/répondant
  - Interface initiateur/répondant
  - Index initiateur/répondant
  - Passerelle initiateur/répondant
  - MAC initiateur/répondant
  - Protocole
  - Vitesse (kbit/s)
  - ID flux
  - Intrusion
  - Virus
  - Logiciels espions
  - Botnet

URL/analyses bloquées pour toute combinaison de :

- URL
- Catégorie URL
- Domaine URL
- Application
- Catégorie de l'application
- Risque de l'application
- Signature
- Action
- IP initiateur/répondant
- Pays initiateur/répondant
- Port initiateur/répondant
- Octets initiateur/répondant
- Interface initiateur/répondant
- Index initiateur/répondant
- Passerelle initiateur/répondant
- MAC initiateur/répondant
- Protocole
  - Vitesse (kbit/s)
  - ID flux
  - Intrusion
  - Virus
  - Logiciels espions
  - Botnet

Analytics Flow Monitor – zoom avant et rotation pour les paramètres de flux

- Applications
  - Noms
  - Catégories
  - Signatures
- Utilisateurs
  - Nom
  - Adresse IP
  - Noms de domaines
  - Types d'authentification
- Activités Web
  - Sites Web
  - Catégories Web
  - URL
- Sources
  - Adresses IP
  - Interfaces
  - Pays
- Destinations
  - Adresses IP
  - Interfaces
  - Pays
- Menaces
  - Intrusions
  - Virus
  - Logiciels espions
  - Spam
  - Botnets
- VoIP
  - Types de médias
  - Identifiants appelants
- Appareils
  - Adresses IP
  - Interfaces
  - Noms
- Contenu
  - Adresses e-mail
  - Types de fichier
- Gestion de la bande passante
  - Entrant
  - Sortant
  - Tout
  - URL
  - Sessions
  - Nombre total de paquets
  - Nombre total d'octets
  - Menaces

Graphiques en étoile – visualisations point à point, zooms avant et rotation

- Sources / Utilisateurs / Emplacements / Appareils
  - De/Vers
    - » Destinations
    - » Applications
    - » Activités Web
    - » Menaces
  - Filtré par
    - » Nombre de connexions
    - » Données transférées
    - » Paquets échangés
    - » Nombre de menaces
  - Halo de mise en évidence pour
    - » Menaces
    - » Données > 1 Mo
    - » Connexions >1000
    - » Paquets >1000

Licences et packages

Capture Security Center (CSC)		Niveau de licence			
		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Licence requise	Disponible pour les clients avec abonnement AGSS/CGSS actif	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Gestion	Écran unique	✓	✓	✓	
	Sauvegarde/Restauration	✓	✓	✓	
	Planification des tâches		✓	✓	
	Gestion groupée des pare-feux		✓	✓	
	Héritage direct et inverse		✓	✓	
	Sans intervention		✓	✓	
	Téléchargement signatures de pare-feu hors ligne		✓	✓	
	Workflow		✓	✓	
Création de rapports	Live Monitor, tableaux de bord récapitulatifs			✓	
	Téléchargements de rapports : applications, menaces, CFS, utilisateurs, trafic, etc.			✓	
	Rapports planifiés			✓	
Analytics	Analytics (conservation 30 jours)				✓
	Cloud App Security (conservation 30 jours)				✓

Informations de commande Capture Security Center

Produit	Référence
SonicWall Capture Security Center Management pour TZ Series, NSv 10 à 100, 1 an	01-SSC-3664
SonicWall Capture Security Center Management pour TZ Series, NSv 10 à 100, 2 ans	01-SSC-9151
SonicWall Capture Security Center Management pour TZ Series, NSv 10 à 100, 3 ans	01-SSC-9152
SonicWall Capture Security Center Management pour NSA 2600 à 6650 et NSv 200 à 400, 1 an	01-SSC-3665
SonicWall Capture Security Center Management pour NSA 2600 à 6650 et NSv 200 à 400, 2 ans	01-SSC-9214
SonicWall Capture Security Center Management pour NSA 2600 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 6650 et NSv 200 à 400, 1 an	01-SSC-3879
SonicWall Capture Security Center Management and Reporting pour NSA 2600 à 6650 et NSv 200 à 400, 2 ans	01-SSC-9154
SonicWall Capture Security Center Management and Reporting pour NSA 2600 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 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 : NSa 2600 à NS*a* 6650 et TZ Series
- Appliances virtuelles de sécurité réseau SonicWall : NSv 10 à NSv 400

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.

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

Datasheet-Analytics-US-VG-MKTG4305