SonicWall Analytics

Transformer les données en informations exploitables

SonicWall Analytics transforme les données de trafic du pare-feu en informations exploitables pour l'ensemble des utilisateurs, applications et réseaux afin d'aider à minimiser les risques de sécurité avec davantage de précision et de rapidité – le tout au sein d'une seule interface. Conçue à partir d'une architecture hautes performances, la machine analytique enrichit une quantité massive de données brutes issues de milliers de nœuds de pare-feu à grande échelle afin d'offrir aux parties prenantes une visibilité intégrale et une sécurité transparente via un tableau de bord exécutif.

Analytics crée des représentations visuelles et de connaissances des ensembles de données en ayant recours à diverses formes de graphiques sémantiques, diagrammes temps/utilisation et tableaux visant à réduire les silos de données et la fatigue des analystes. Grâce à des capacités de zoom supplémentaires, les responsables de la sécurité peuvent examiner et se concentrer sur les points de données essentiels afin **d'exposer les risques cachés pour une intervention précoce** et prendre des mesures stratégiques étayées par des données contre les activités à risque des utilisateurs au fur et à mesure qu'ils progressent dans la procédure de découverte.

Forts d'une visibilité et d'un contrôle complets, les analystes de la sécurité voient tout partout et deviennent de meilleurs gestionnaires des risques. Les répondants quant à eux peuvent consacrer leur précieux temps et leurs efforts à l'orchestration de mesures rapides au niveau des applications et utilisateurs essentiels plutôt que de réagir à chaque événement. Analytics offre **l'agilité et l'élasticité du cloud** pour satisfaire aux exigences les plus strictes des entreprises.

AVANTAGES

Entreprise

- Bénéficiez d'une transparence intégrale sur la sécurité
- Obtenez un instantané en temps réel de votre stratégie de sécurité
- Remplissez vos obligations internes de conformité
- Effectuez une planification et une budgétisation précises de votre cyberdéfense
- Réduisez les dépenses d'investissement et les coûts d'exploitation

Exploitation

- Comprenez facilement et d'emblée les métriques de la sécurité
- Bénéficiez d'informations issues de chaque réseau, événement utilisateur et alerte
- Instaurez avec précision des actions stratégiques défensives
- Évoluez et bénéficiez de l'agilité et de l'élasticité du cloud

Sécurité

- Identifiez les risques cachés
- Garantissez une intervention précoce
- Réagissez à temps aux activités dangereuses des utilisateurs
- Aidez les analystes à devenir de meilleurs gestionnaires de risques
- Aidez les répondants à mieux solutionner les problèmes

En savoir plus sur SonicWall Analytics

www.sonicwall.com/analytics

FICHE TECHNIQUE

Tout voir, partout

Analytics vous apporte une vue complète de l'ensemble de votre environnement de sécurité SonicWall au niveau des détenteurs d'accès, des groupes ou des appareils. Le tableau de bord exécutif affiche une surveillance et une analyse statiques et quasiment en temps réel de l'ensemble du trafic réseau et de la communication de données passant par l'écosystème du pare-feu. Toutes les données de journaux sont enregistrées, agrégées, mises en contexte et synthétisées de manière claire et facilement exploitable pour vous permettre de découvrir, d'interpréter, de trier et de prendre les mesures défensives nécessaires sur la base de données étayées.

Analytics intègre une vaste sélection de rapports prédéfinis qui peuvent être fournis à la demande ou planifiés de façon régulière. Il offre également la flexibilité requise pour créer des rapports personnalisés avec les valeurs et les métriques choisies dans une vaste bibliothèque de types de données de pare-feu, ce qui vous permet d'assembler et d'extraire de façon logique de précieuses informations depuis des appareils spécifiques dans les groupes ou les détenteurs d'accès sélectionnés. Les rapports personnalisés contribuent à désengorger les entonnoirs de données, ce qui offre aux décideurs et aux répondants la visibilité et les

Figure 1.0 Tableau de bord exécutif

informations exploitables requises sur des ensembles de données plus petits mais plus qualitatifs pour l'analyse de trafic, les lacunes de sécurité et la détection d'anomalies. Ils peuvent ainsi zoomer sur l'analyse appropriée, prendre des décisions éclairées et mener des actions stratégiques au bon moment sur la base de données fiables.

Comprendre votre risque

Les fonctionnalités de zoom avant et de rotation vous permettent d'examiner plus en détail et avec plus de certitude les schémas et tendances spécifiques associés au trafic d'entrée et de sortie, l'utilisation des applications, l'accès des utilisateurs et des appareils, les actions face aux menaces, etc. Grâce à la combinaison de rapports et d'analyses des endpoints, réseaux, utilisateurs et applications, vous pouvez faire des analyses de manière proactive et réagir aux alertes, anomalies et activités dangereuses des utilisateurs. Grâce à une sécurité entièrement transparente, vous bénéficiez d'une perception optimale de la situation afin de détecter les risques pour la sécurité, d'orchestrer les actions stratégiques, d'instaurer une stratégie de sécurité cohérente et de surveiller en continu les résultats pour l'ensemble de l'environnement.

Optimiser la productivité de vos employés

User Analytics vous offre une visibilité globale et transparente de l'utilisation par vos employés des applications Web et d'Internet. Grâce à des capacités de zoom, les analystes sont en mesure d'analyser les points de données intéressants et d'établir des mesures étayées et conformes aux règles en lien avec les utilisateurs et applications à risque au fur et à mesure du processus de découverte. En outre, Productivity Reports met à votre disposition des informations relatives à l'utilisation d'Internet et au comportement en ligne de vos employés sur une période déterminée. Cette fonction génère des instantanés performants ou des rapports détaillés vous permettant de classer les activités en ligne des utilisateurs dans différents groupes de productivité (productif, improductif, acceptable, inacceptable ou personnalisé) afin d'aider l'organisation à mieux comprendre et contrôler l'utilisation d'Internet.

Déploiement flexible avec les options SaaS, virtuelle ou IaaS

Analytics vous offre plusieurs possibilités de déploiement flexibles pour répondre au mieux à vos besoins opérationnels.

Pour une expérience ne nécessitant pas de maintenance, Analytics est intégré à l'offre SaaS NSM (Network Security Manager) hébergée par SonicWall et accessible sur Internet. L'option SaaS vous offre une élasticité illimitée pour évoluer à la demande tout en limitant vos coûts d'exploitation. Les coûts habituellement associés à l'acquisition du matériel et des logiciels, à l'installation personnalisée, aux maintenances et mises à jour régulières, à l'amortissement des installations et à leur retrait de service sont supprimés et remplacés par un coût d'abonnement annuel moindre et prévisible.

Pour un contrôle et une conformité absolus de votre système, vous pouvez déployer Analytics sur site sous forme de logiciel installé sur la plateforme virtuelle de votre choix, p. ex. VMWare. Vous bénéficiez ainsi de tous les avantages opérationnels et économiques de la virtualisation, notamment l'évolutivité du système, la mise à disposition rapide des systèmes et la réduction des coûts.

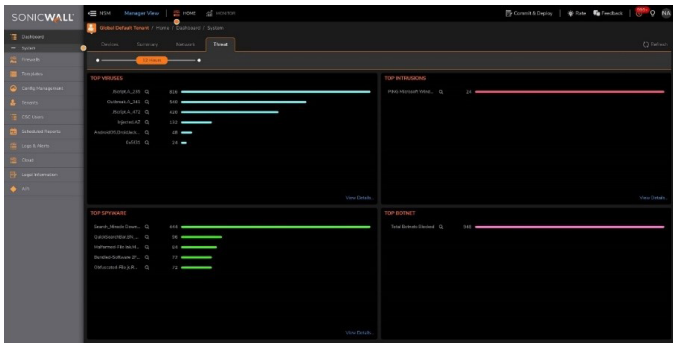

Figure 2.0 Résumé des menaces

Récapitulatif des fonctionnalités

Fonctionnalité	Description
Analyses utilisateur	Vue complète du réseau du personnel, des applications et des activités des menaces depuis un tableau de bord interactif. Vous pouvez zoomer au niveau granulaire sur les archives historiques afin d'instaurer des mesures étayées et conformes aux stratégies contre les activités en ligne dangereuses des utilisateurs.
Analyse du trafic applicatif	Fournissez 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.
Analyse de la sécurité	Bénéficiez d'une visibilité en temps réel avec détection rapide des menaces. Permettez aux analystes de la sécurité et aux responsables en cas d'incidents de traquer, d'identifier et d'examiner les problèmes.
Visualisation dynamique en temps réel	Sur un seul et même écran, les analystes de la sécurité peuvent réaliser des analyses approfondies avec zoom pour examiner les données de sécurité avec davantage de précision et de rapidité.
Rapidité de détection et d'élimination	Des fonctionnalités d'investigation suivent les activités dangereuses et gèrent rapidement les risques en vue de les éliminer grâce à des mesures appropriées.
Rapports de productivité	Communiquez des informations sur l'utilisation des ressources Internet de l'organisation. Génération d'instantanés performants et de rapports d'analyse approfondis sur le comportement d'accès des utilisateurs à Internet.

Fonctionnalité	Description
Rapports personnalisés	Workflow auto-guidé ou rapports personnalisés avec des valeurs et des métriques choisies dans une bibliothèque de types de données de pare-feu.
Rapports niveau détenteur d'accès ou groupe	Permet aux utilisateurs d'afficher des rapports prédéfinis ou personnalisés au niveau de l'appareil ou du détenteur d'accès.
Rapports VPN	Synthèse des ressources d'entreprise utilisées dans le tunnel VPN, de la bande passante consommée et des utilisateurs (c'est-à-dire nom d'utilisateur et adresse IP) du trafic. Les administrateurs réseau peuvent exploiter ces informations pour surveiller les applications vitales, contrôler ou gérer le trafic et planifier la croissance des capacités.
Analyse et reporting sur les flux	Fournissez 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 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 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 le zoom avant détaillé de sessions et de paquets
Rapports graphiques exhaustifs	Visibilité sur les menaces au niveau du pare-feu, l'utilisation de la bande passante, la productivité des employés, les activités réseau suspectes et l'analyse du trafic des applications.
Reporting Syslog (uniquement pour Analytics 2.5)	Rationalisez la synthèse des données pour un reporting quasiment en temps réel des messages entrants Syslog. L'accès direct aux données brutes sous-jacentes augmente encore la précision et les options de personnalisation des rapports.
Rapports planifiés	Permet la centralisation de tous les rapports planifiés. Un rapport peut combiner les graphiques et les tableaux de plusieurs appareils. Les rapports peuvent être planifiés et envoyés sous divers formats à un ou plusieurs analyste(s).
Affichage « en un coup d'œil »	Offre des vues personnalisables pour illustrer plusieurs rapports synthétiques sur une même page, ce qui permet aux utilisateurs d'accéder facilement aux paramètres clés du réseau et de procéder à des analyses rapides à partir des données disponibles.
Rapports multi-menaces	Collectez des informations sur les attaques et observez instantanément l'activité des menaces détectées par les pare-feux SonicWall à l'aide de SonicWall Capture ATP, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention et Application Intelligence and Control Service.
Fonctions intelligentes d'analyse des attaques	Comptes-rendus sur certains types d'attaques, tentatives d'intrusion, ainsi que sur leur adresse d'origine permettant aux administrateurs de répondre rapidement à l'arrivée de nouvelles menaces.
Rapports sur les points d'accès sans fil sauvages	Affichage de tous les appareils sans fil en cours d'utilisation ainsi que du 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.
Rapport Capture ATP	Fournit un tableau de bord concis de l'analyse des menaces, ainsi que des rapports détaillant les résultats d'analyse des fichiers envoyés au service, à savoir source, destination et récapitulatif ainsi que les détails relatifs à l'action des programmes malveillants une fois déclenchés.
Rapport sur les botnets	Il existe quatre types de rapports : Tentatives, Cibles, Initiateurs et Chronologie, contenant le contexte du vecteur de l'attaque, p. 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.
Journalisation centralisée	Offre un emplacement centralisé pour consolider les événements de sécurité et les journaux de toutes les appliances gérées, ce qui permet de réaliser des analyses forensiques du réseau à partir d'un point unique.
Architecture cloud native	Collectez, combinez, traitez, retraitez, extrayez, corrélez et chargez d'énormes quantités de données interrogées depuis des dizaines de milliers de nœuds de pare-feu en bénéficiant de la rapidité et de l'élasticité du cloud.

Licences et packages

Création de rapports				
Fonctionnalités	SaaS Analytics pour NSM Essential	SaaS Analytics pour NSM Essential	Analyse sur site	Analyse sur site
Protocole de journalisation	basé sur Netflow/ IPFIX[1]	basé sur Netflow/ IPFIX[1]	basé sur Netflow/ IPFIX[1]	basé sur Syslog[1]
Tableau de bord niveau groupe/détenteur d'accès	Oui	Oui	Non	Non
Capture ATP (niveau appareil)	Oui	Oui	Oui	Oui
Capture Threat Assessment (CTA) (niveau appareil)	Oui	Oui	Oui	Non
Rapports de productivité[3]	Non	Oui	Non	Non
Rapports VPN	Non	Oui	Non	Oui
Rapport personnalisé	Non	Oui	Oui	Oui
Rapport planifié (Flow, Syslog, CTA ou Management)	Oui (sauf Flow)	Oui	Oui	Oui
Jours de données de reporting	7 jours	365 jours	365 jours	365 jours
Analytics				
Jours de données de reporting	-	30 jours	90 jours	90 jours
Analyse selon utilisateur	Non	Oui	Oui	Oui
Analyse des applications	Non	Oui	Oui	Oui
Analyse forensique réseau et chasse aux menaces avec zooms avant et rotations	Non	Oui	Oui	Oui
Support technique	Support 24h/24, 7j/7	Support 24h/24, 7j/7	Support 24h/24, 7j/7[2]	Support 24h/24, 7j/7[2]

[1] Nécessite un service AGSS/CGSS ou un service payé Capture Security Center
[2] Nécessite une licence de support 24 h/24, 7 j/7
[3] Nécessite une licence AGSS/CGSS activée sur les pare-feux de génération 6/6.5, une licence Essential Protection sur les pare-feux de génération 7

Configuration minimum requise

Pour la version SaaS de SonicWall Analytics via Network Security Manager :

Appliances SonicWall prises en charge

- Appliances de sécurité réseau SonicWall : appliances série NSA, série NS*a*, série TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliances virtuelles de sécurité réseau SonicWall : NS*v* 10 à NS*v* 400

Firmware SonicWall pris en charge

- SonicWall SonicOS 6.0 ou version supérieure

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)

Pour un déploiement de SonicWall Analytics sur site :

Appliance virtuelle

- Hyperviseur : VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- Mémoire vive recommandée : sans limite (8 Go minimum)
- Disque dur : Base OVA 65 Go (montage externe)
- vCPU : 4/sans limite
- Interface réseau : 1
- Guide de compatibilité VMware

Firmware SonicWall pris en charge

- SonicWall SonicOS 6.0 ou version supérieure

Appliances SonicWall prises en charge

- Appliances de sécurité réseau SonicWall : appliances série NS*sp*, série SuperMassive E10000 et 9000, série NSA, série NS*a*, série TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliances virtuelles de sécurité réseau SonicWall : Série NS*v* 10

En savoir plus sur SonicWall Analytics

www.sonicwall.com/analytics

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, consultez notre site à l'adresse : www.sonicwall.com.

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

© 2023 SonicWall Inc. TOUS DROITS RÉSERVÉS.
SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives. Les informations contenues dans ce document sont fournies en relation avec les produits de SonicWall et/ou ses filiales. Aucune licence, expresse ou implicite, par estoppel ou un autre moyen, quant à un quelconque droit de propriété intellectuelle n'est accordée par le présent document ou en lien avec la vente de produits SonicWall. Sauf disposition contraire dans les conditions du contrat de licence, la société SonicWall et/ou ses filiales déclinent toute responsabilité quelle qu'elle soit et rejettent toute garantie expresse, implicite ou statutaire concernant leurs produits, y compris et sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier ou de non-contrefaçon. En aucun cas, SonicWall et/ou ses filiales ne seront responsables des dommages directs, indirects, consécutifs, punitifs, spéciaux ou fortuits (y compris, sans limitation, les dommages pour perte de profits, interruption de l'activité ou perte d'informations) provenant de l'utilisation ou l'impossibilité d'utiliser ce document, même si SonicWall et/ou ses filiales ont été informés de l'éventualité de tels dommages. SonicWall et/ou ses filiales ne font aucune déclaration ou ne donnent aucune garantie en ce qui concerne l'exactitude ou l'exhaustivité du contenu de ce document et se réservent le droit d'effectuer des changements quant aux spécifications et descriptions des produits à tout moment sans préavis. SonicWall Inc. et/ou ses filiales ne s'engagent en aucune mesure à mettre à jour les informations contenues dans le présent document.

Datasheet-Analytics-A4-JK-8806