SonicWall Analytics

Transformación de datos en información valiosa accionable

SonicWall Analytics transforma los datos del tráfico de los firewalls en información valiosa accionable para todos los usuarios, aplicaciones y redes con el fin de ayudar a mitigar los riesgos de seguridad con mayor precisión y velocidad - todo ello a través de una única interfaz. Basado en una arquitectura de alto rendimiento, el motor de análisis enriquece una enorme cantidad de datos sin procesar en miles de nodos de firewall a escala para proporcionar a las partes interesadas una visibilidad completa y transparencia de la seguridad a través de un dashboard ejecutivo.

Analytics crea representaciones visuales y del conocimiento de los conjuntos de datos utilizando diversas formas de gráficos semánticos, así como diagramas y tablas de tiempo-uso para ayudar a reducir los silos de datos y la fatiga de los analistas. Gracias a las prestaciones adicionales de desglose, los encargados de responder a los incidentes de seguridad pueden investigar y centrarse en los puntos de datos críticos con el fin de **exponer riesgos ocultos para una intervención temprana,** así como emprender acciones probadas basadas en políticas contra las actividades peligrosas de los usuarios a medida que se detectan en el proceso de descubrimiento.

Con una visibilidad y un control exhaustivos, los analistas de seguridad pueden ver todo en todos lados para gestionar mejor los riesgos, mientras los responsables de responder a los incidentes pueden dedicar su valioso tiempo a orquestar acciones de respuesta rápidas para las aplicaciones y los usuarios más importantes, en lugar de tener que reaccionar a cada evento. Analytics es escalable y ofrece la **agilidad y la elasticidad de la tecnología de nube** para cumplir incluso los requisitos más exigentes de las empresas.

PRESTACIONES DESTACADAS

Empresa

- Disfrute de total transparencia de la seguridad
- Obtenga una instantánea del estado de seguridad en tiempo real
- Cumpla las normas internas
- Elabore planes y presupuestos de ciberdefensa precisos
- Reduzca los gastos operativos y de capital

Operaciones

- Entienda fácilmente los parámetros de seguridad de un vistazo
- Obtenga información valiosa de cada evento y alerta de la red y los usuarios
- Establezca acciones defensivas precisas basadas en políticas
- Escale y actúe con la agilidad y elasticidad de la tecnología de nube

Seguridad

- Descubra riesgos ocultos
- Permita la intervención temprana
- Responda en el momento oportuno a las actividades de riesgo de los usuarios
- Ayude a los analistas a gestionar mejor los riesgos
- Ayude a los responsables de responder a los incidentes de seguridad a solucionar mejor los problemas

Obtenga más información sobre SonicWall Analytics

www.sonicwall.com/analytics

FICHA TÉCNICA

Vea todo en todos lados

Analytics le proporciona una visión completa de todo su entorno de seguridad de SonicWall a nivel del tenant, grupo o dispositivo. El dashboard ejecutivo proporciona monitorización estática y casi en tiempo real de los riesgos, así como análisis de todo el tráfico de red y de todos los datos que pasan por el ecosistema del firewall. Todos los datos de registro se registran, agregan, contextualizan y presentan de forma significativa y fácilmente consumible, para que usted pueda descubrir, interpretar, cribar y tomar las medidas defensivas necesarias en base a la información extraída de los datos.

Figura 1.0 Dashboard ejecutivo

Analytics viene con una amplia variedad de informes predefinidos que pueden entregarse bajo demanda o de forma regular. Asimismo, le brinda la flexibilidad necesaria para crear informes personalizados con valores y parámetros elegidos de una extensa biblioteca de tipos de datos de firewall, lo cual le permite ensamblar y extraer de forma lógica información valiosa desde dispositivos específicos en grupos o tenants seleccionados. Los informes personalizados ayudan a despejar los cuellos de botella de datos, proporcionando a los responsables de la toma de decisiones una visibilidad más clara e inteligencia accionable desde conjuntos de datos más pequeños, pero de mayor calidad, para el análisis del tráfico y la detección de brechas de seguridad y anomalías. Ahora, pueden centrarse en los análisis adecuados, tomar decisiones informadas y emprender acciones basadas en políticas en base a datos fiables en el momento oportuno.

Conozca su riesgo

Las prestaciones de desglose y rotación le permiten examinar más detalladamente patrones específicos y tendencias relacionados con el tráfico entrante/saliente, el uso de las aplicaciones, el acceso de los usuarios y dispositivos, acciones de amenazas etc. con confianza. Utilizando una mezcla de informes y análisis de los endpoints, la red, los usuarios y las aplicaciones, puede analizar o responder proactivamente a las alertas, anomalías y actividades de riesgo de los usuarios. La total transparencia de la seguridad le proporcionará conocimiento situacional para descubrir los riesgos de seguridad, orquestar las acciones basadas en políticas, impulsar el refuerzo consistente de la seguridad y monitorizar continuamente los resultados en todo su entorno.

Optimice la productividad del personal

Los Análisis de usuarios proporcionan una vista amplia y transparente de las actividades de uso de aplicaciones Web e Internet por parte de sus empleados. Las prestaciones de desglose permiten a los analistas rotar e investigar los puntos de datos de interés y establecer medidas controladas por políticas y respaldadas por pruebas para los usuarios y las aplicaciones de riesgo a medida que se detectan en el proceso de descubrimiento. Además, la función de Informes de productividad proporciona información valiosa sobre el uso de Internet por parte de los empleados, así como sobre su comportamiento, durante un determinado periodo. Genera potentes instantáneas o informes detallados que clasifican las actividades Web de los usuarios en grupos de productividad, como productivas, improductivas, aceptables, inaceptables, y grupos personalizados, ayudando a las organizaciones a entender y a controlar mejor el uso de Internet.

Implementación flexible con opciones SaaS, virtual o IaaS

Analytics le ofrece opciones flexibles de implementación que se ajustan al máximo a sus requisitos operacionales.

A fin de ofrecer una experiencia libre de mantenimiento, Analytics está integrado en SonicWall Network Security Manager (NSM) SaaS, hospedado por SonicWall, y es accesible por Internet. Esta opción le brinda una elasticidad ilimitada y escalabilidad bajo demanda, al tiempo que reduce sus costes operacionales. Se eliminan los habituales costes de adquisición de hardware y software, instalación personalizada, mantenimiento y actualizaciones regulares, depreciación de activo y retirada, y se sustituyen por un reducido coste de suscripción anual predecible.

Para disfrutar de un control total y garantizar el cumplimiento normativo, puede implementar Analytics on-prem como software instalado en la plataforma virtual que usted elija, como VMWare. Se beneficiará de todas las ventajas operativas y económicas de la virtualización, como la escalabilidad de los sistemas, la velocidad de aprovisionamiento de los sistemas y la reducción de costes.

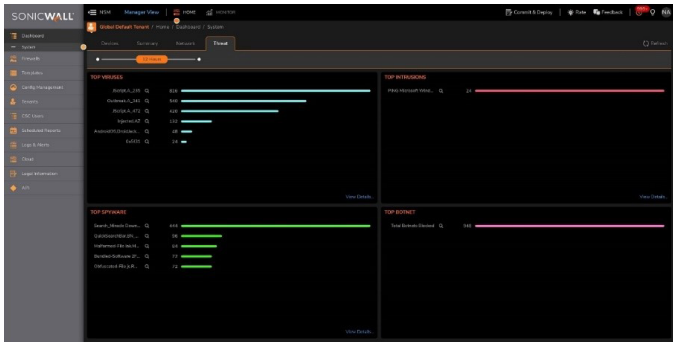

Figura 2.0 Resumen de las amenazas

Resumen de las prestaciones

Prestación	Descripción
Análisis de usuarios	Muestre una visión completa de las actividades del personal en relación con la red, las aplicaciones y las amenazas mediante un dashboard interactivo. Puede desglosar granularmente los registros históricos para establecer medidas controladas por políticas y respaldadas por pruebas contra actividades Web de riesgo por parte de los usuarios.
Análisis del tráfico de aplicaciones	Ofrecen a las organizaciones una visión transparente del tráfico de aplicaciones, el uso del ancho de banda y las amenazas de seguridad, así como potentes prestaciones de análisis forenses y resolución de problemas.
Análisis de seguridad	Obtenga visibilidad en tiempo real con detección rápida de amenazas. Permita a los analistas de seguridad y a los encargados de responder a los incidentes detectar, identificar e investigar problemas.
Visualización dinámica en tiempo real	Mediante una única consola, los analistas de seguridad pueden llevar a cabo análisis forenses y de investigación profundos y detallados de los datos de seguridad con mayor precisión y velocidad.
Detección y resolución rápidas	Tecnología de investigación para perseguir actividades peligrosas y para gestionar y remediar riesgos rápidamente tomando medidas adecuadas.
Informes de productividad	Proporcione información valiosa sobre el uso de los recursos de Internet en la organización. Genera potentes instantáneas e informes con funciones de desglose sobre el comportamiento de acceso a Internet por parte de los usuarios.

Prestación	Descripción
Informes personalizados	Flujo de trabajo autoguiado para crear informes personalizados con valores y parámetros seleccionados de una biblioteca de tipos de datos de firewall.
Informes a nivel de tenant y de grupo	Permita a los usuarios ver informes predefinidos o personalizados a nivel de grupo de dispositivos o de tenant.
Informes de VPN	Ofrecen un resumen de los recursos de la empresa que se están utilizando en el túnel VPN, cuánto ancho de banda se está consumiendo y quién (nombre de usuario y dirección IP) utiliza ese tráfico. Los administradores de red pueden utilizar esta información para monitorizar las aplicaciones críticas de negocio, controlar o dar forma al tráfico y planificar el crecimiento de la capacidad.
Análisis e informes de flujos	Proporcionan un agente de informes de flujos para el análisis del tráfico de las aplicaciones, así como datos sobre el uso mediante protocolos IPFIX o NetFlow a fin de ofrecer una monitorización en tiempo real e histórica. Ofrecen a los administradores una interfaz efectiva y eficiente para monitorizar visualmente su red en tiempo real. De esta forma, pueden identificar aplicaciones y páginas Web con gran demanda de ancho de banda, visualizar el uso de las aplicaciones por usuarios y anticiparse a ataques y amenazas en la red. • Una pantalla de informes en tiempo real con filtrado de un solo clic • Un dashboard de los flujos principales con botones de "Visualizar por" de un solo clic • Una pantalla de informes de flujos con pestañas de atributos de flujos adicionales • Una pantalla de análisis de flujos con potentes funciones de correlación y dinamización • Un visor de sesiones para el desglose profundo de sesiones individuales y paquetes
Informes gráficos exhaustivos	Proporcionan visibilidad de las amenazas del firewall, el uso del ancho de banda, la productividad de los empleados, la actividad de red sospechosa y el análisis del tráfico de las aplicaciones.
Informes Syslog (Solo para Analytics 2.5)	Optimizan el resumen de los datos, permitiendo la elaboración de informes casi en tiempo real de los mensajes Syslog entrantes. El acceso directo a los datos brutos subyacentes mejora todavía más la granularidad y las opciones de personalización de los informes.
Informes programados	Proporcionan un punto de entrada único para todos los informes programados. Los informes pueden contener diagramas y tablas de múltiples unidades. Los informes pueden programarse y enviarse a uno o más analistas en diferentes formatos.
Informes de un solo vistazo	Ofrecen una visión personalizable con múltiples informes resumidos en una sola página. Los usuarios pueden acceder fácilmente a la información crítica de la red para analizar los datos rápidamente a través de múltiples informes.
Informes sobre amenazas múltiples	Recopilan información acerca de ataques y permiten acceder de forma inmediata a la información sobre las amenazas detectadas por los firewalls SonicWall utilizando SonicWall Capture ATP y Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service.
Nuevas funciones de inteligencia de ataques	Ofrecen informes sobre determinados tipos de ataques o intentos de intrusión y detectan la dirección de origen del ataque, permitiendo a los administradores responder rápidamente ante cualquier amenaza activa.
Informes de puntos de acceso inalámbricos no autorizados	Muestran todos los dispositivos inalámbricos que se están utilizando, así como el comportamiento no autorizado de las interconexiones punto a punto ad hoc entre hosts y asociaciones accidentales de usuarios que se conectan a redes vecinas no autorizadas.
Informe de Capture ATP	Proporciona informes y un dashboard de análisis de amenazas de un solo vistazo con información detallada sobre los resultados del análisis de los archivos enviados al servicio (origen, destino y un resumen con detalles de la acción del malware tras su detonación).
Informe botnet	Incluye cuatro tipos de informes: Intentos, objetivos, iniciadores e intervalos de tiempo, que incluyen contextos de vectores de ataque, como ID de botnet, direcciones IP, países, hosts, puertos, interfaces, iniciador/objetivo, origen/destino y usuario.
Informe de Geo IP	Contiene información sobre el tráfico bloqueado en base al país de origen o destino del tráfico. Incluye cuatro tipos de informes: Intentos, objetivos, iniciadores e intervalos de tiempo, que incluyen contexto de vectores de ataque, como ID de botnet, direcciones IP, países, hosts, puertos, interfaces, iniciador/objetivo, origen/destino y usuario.
Protocolización centralizada	Proporciona un punto central para consolidar los eventos de seguridad y protocolos de todos los dispositivos gestionados, permitiendo realizar los análisis forenses de la red desde un único punto.
Arquitectura nativa de nube	Recopila, combina, procesa, reprocesa, extrae, correlaciona y carga enormes cantidades de datos consultados de decenas de millares de nodos de firewall con velocidad y elasticidad de nube.

Licencias y paquetes

Informes				
Prestaciones	Analytics SaaS para NSM Essential	Analytics SaaS para NSM Advanced	Analytics local	Analytics local
Protocolo de registro	Basado en NetFlow/ IPFIX[1]	Basado en NetFlow/ IPFIX[1]	Basado en NetFlow/ IPFIX[1]	Basado en Syslog[1]
Dashboard de nivel de grupo/tenant	Sí	Sí	No	No
Capture ATP (Nivel de dispositivo)	Sí	Sí	Sí	Sí
Capture Threat Assessment (CTA) - Nivel de dispositivo	Sí	Sí	Sí	No
Informes de productividad[3]	No	Sí	No	No
Informes de VPN	No	Sí	No	Sí
Informes personalizados	No	Sí	Sí	Sí
Planificación de informes (Flujos, Syslog, CTA o gestión)	Sí (excepto flujos)	Sí	Sí	Sí
Días de datos de informes	7 días	365 días	365 días	365 días
Análisis				
Días de datos de análisis	-	30 días	90 días	90 días
Análisis basado en usuarios	No	Sí	Sí	Sí
Análisis de aplicaciones	No	Sí	Sí	Sí
Análisis forenses de la red y caza de amenazas utilizando funciones de desglose de datos y de rotación	No	Sí	Sí	Sí
Soporte técnico	Soporte 24x7	Soporte 24x7	Soporte 24x7[2]	Soporte 24x7[2]

[1] Requiere servicio AGSS/CGSS o cualquier servicio de pago de Capture Security Center
[2] Requiere una licencia de soporte 24x7
[5] Requiere licencia AGSS/CGSS en firewalls de generación 6/6.5, licencia Essential Protection en firewalls de 7ª generación.

Requisitos mínimos del sistema

Para SonicWall Analytics en modo SaaS vía Network Security Manager:

Dispositivos SonicWall soportados:

- Dispositivos SonicWall de seguridad de red: Dispositivos de las series NSA, NS*a*, TZ, SOHO-W, SOHO 250, SOHO 250W
- Dispositivos virtuales de seguridad de red de SonicWall: NS*v* 10 a NS*v* 400

Firmware SonicWall soportado

- SonicWall SonicOS 6.0 o superior

Navegadores de Internet

- Microsoft® Internet Explorer 11.0 o superior (no utilizar modo de compatibilidad)
- Mozilla Firefox 37.0 o superior
- Google Chrome 42.0 o superior; Safari (última versión)

Para la implementación local de SonicWall Analytics:

Dispositivo virtual

- Hipervisor: VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- RAM recomendada: Ilimitada (8 GB mínimo)
- Disco duro: Base OVA 65 GB requiere montaje externo
- vCPU: 4/ilimitada
- Interfaz de red: 1
- Guía de compatibilidad de VMware

Firmware SonicWall soportado

- SonicWall SonicOS 6.0 o superior

Dispositivos SonicWall soportados:

- Dispositivos SonicWall de seguridad de red: Series NS*sp*, SuperMassive E10000 y 9000, serie NSA, serie NS*a*, dispositivos de la serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Dispositivos virtuales de seguridad de red de SonicWall: Serie NS*v*

Obtenga más información sobre SonicWall Analytics

www.sonicwall.com/analytics

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-Analytics-A4-JK-8806