SonicWall Analytics

Transforma los datos en información, la información en conocimiento, el conocimiento en decisiones y las decisiones en acciones

SonicWall Analytics le brinda una visión global y detallada de lo que ocurre dentro del entorno de seguridad de red de SonicWall. Y todo a través de una única consola. En su núcleo dispone de un motor de análisis potente basado en inteligencia que automatiza la agregación, normalización, correlación y contextualización de los datos de seguridad que fluyen por todos los firewalls de SonicWall y los puntos de acceso inalámbricos. El dashboard interactivo de la aplicación utiliza varias formas de gráficos y tablas de tiempo-uso para crear representaciones de los modelos de datos.

Analytics muestra los resultados en un formato significativo, accionable y de fácil acceso. Esto permite a los equipos de seguridad, analistas, auditores, órganos de decisión y directivos interpretar, priorizar, tomar decisiones basadas en hechos, y tomar medidas defensivas y correctivas adecuadas contra riesgos y amenazas conforme van apareciendo en el proceso de descubrimiento.

Analytics facilita a los interesados una visibilidad detallada en tiempo real y en una única consola, entidad y flexibilidad. De este modo, pueden realizar análisis forenses y de investigación profundos y detallados del tráfico de red, del acceso de usuarios, de la conectividad, aplicaciones y utilización, estado de los recursos de seguridad, eventos de seguridad, perfiles de amenazas y otros datos relacionados con el firewall.

Ventajas:

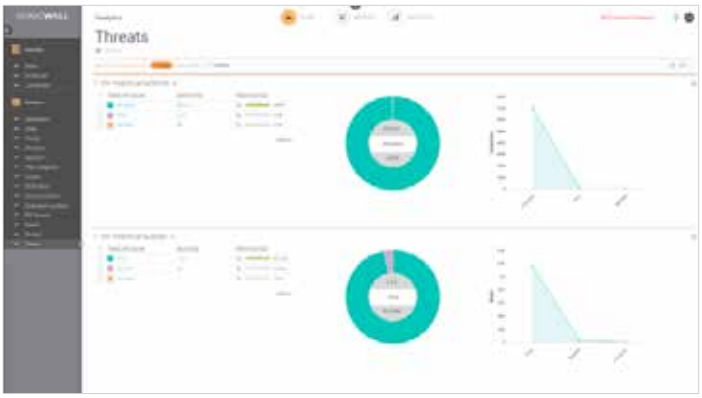
- Obtenga toda la información necesaria y un conocimiento situacional completo del entorno de seguridad de red en una única consola.
- Disfrute de la autoridad y flexibilidad necesarias para llevar a cabo análisis forenses y de investigación en profundidad.
- Consiga un conocimiento y una comprensión más profundos de los riesgos y las amenazas potenciales y reales.
- Remedie los riesgos con mayor claridad, certeza y velocidad.
- Reduzca el tiempo de respuesta a incidentes con inteligencia de amenazas accionable en tiempo real.

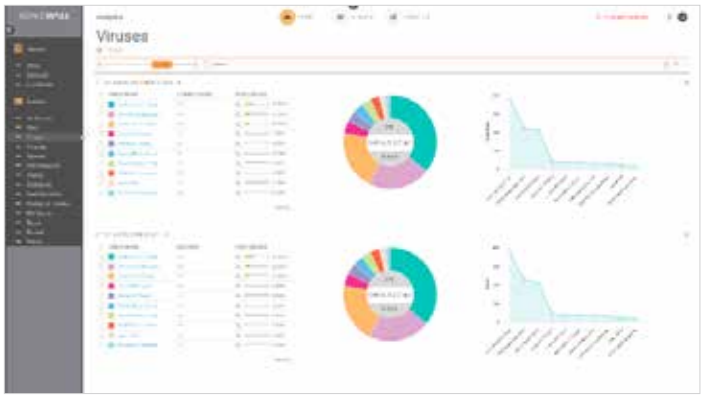
Partner Enabled Services

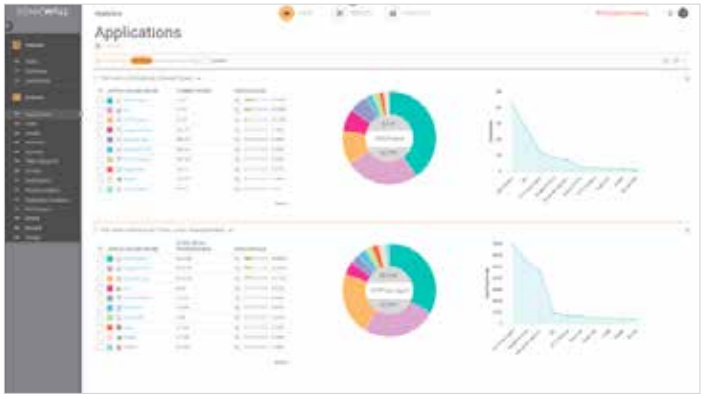
¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

Este conocimiento profundo y esta comprensión del entorno de seguridad proporcionan la inteligencia y la capacidad no solo de descubrir los riesgos de seguridad, sino también de orquestar las medidas necesarias para remediarlos. Asimismo, permiten monitorizar y llevar un seguimiento de los resultados con mayor claridad, certeza y velocidad.

La integración de Analytics en los procesos de negocio ayuda a poner en práctica el análisis, transformando así los datos en información, la información en conocimiento y el conocimiento en decisiones para conseguir la automatización de la seguridad.







Prestaciones de gestión y supervisión de la seguridad	
Prestación	Descripción
Gestión centralizada de la seguridad y de la red	Ayuda a los administradores a implementar, gestionar y supervisar un entorno de seguridad de red distribuido.
Configuración federada de políticas	Establece políticas fácilmente desde una ubicación central para miles de firewalls, puntos de acceso inalámbricos, dispositivos de seguridad de correo electrónico, acceso remoto seguro y switches de SonicWall.
Gestión y flujo de trabajo de las solicitudes de cambio	Esta prestación garantiza la corrección y el cumplimiento de las modificaciones de políticas reforzando un proceso riguroso para la configuración, comparación, validación, revisión y aprobación de políticas antes de la implementación. Los usuarios pueden configurar los grupos de aprobación para cumplir la política de seguridad de la empresa. Todos los cambios de las políticas se registran de forma auditable, garantizándose así que el firewall cumpla con la normativa vigente. Todos los detalles granulares de cualquier cambio realizado se archivan de forma histórica para facilitar el cumplimiento normativo, el seguimiento y la resolución de problemas.
Implementación sin necesidad de intervención	Simplifica y acelera la implementación y el aprovisionamiento de firewalls de SonicWall de forma remota utilizando la nube. Automáticamente implementa políticas, lleva a cabo actualizaciones de firmware y sincroniza licencias.
Despliegue y configuración de VPN eficientes	Ahora, los switches de la serie X de Dell pueden gestionarse fácilmente desde los firewalls de las series TZ, NSA y SuperMassive para ofrecer una única consola desde la cual gestionar toda la infraestructura de seguridad de red.
Gestión fuera de línea	Simplifica y acelera la implementación y el aprovisionamiento de firewalls de SonicWall de forma remota utilizando la nube. Automáticamente implementa políticas, lleva a cabo actualizaciones de firmware y sincroniza licencias.
Gestión de licencias optimizada	Permite habilitar la conectividad VPN de forma sencilla y consolidar miles de políticas de seguridad.
Dashboard universal	Incluye widgets personalizables, mapas geográficos e informes centrados en el usuario.
Supervisión activa de dispositivos y alertas	Proporciona alertas en tiempo real con prestaciones de supervisión integradas. Simplifica la resolución de problemas, ya que permite a los administradores tomar medidas de precaución y aplicar medidas correctivas de forma inmediata.
Soporte SNMP	Proporciona *traps* eficaces en tiempo real para todos los dispositivos y aplicaciones que soportan el Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP) y SNMP, lo que facilita enormemente los esfuerzos de resolución de problemas por identificar los eventos críticos de la red y reaccionar ante ellos.
Visualización e inteligencia de aplicaciones	Ofrece informes históricos y en tiempo real sobre las aplicaciones que se están utilizando y los usuarios que las utilizan. Los informes son completamente personalizables mediante prestaciones intuitivas de filtrado y desglose.
Múltiples opciones de integración	Incluye una interfaz de programación de aplicaciones (API) para servicios Web, compatibilidad con interfaz de línea de comandos (CLI) para la mayoría de las funciones, así como compatibilidad con *trap* SNMP para proveedores de servicios y empresas.
Gestión de switches de la serie Dell Networking X	Ahora, los switches de la serie X de Dell pueden gestionarse fácilmente desde los firewalls de las series TZ, NSA y SuperMassive para ofrecer una única consola desde la cual gestionar toda la infraestructura de seguridad de red.
Informes sobre las normas HIPPA, PCI y SOX	Incluye plantillas predefinidas de informes sobre las normas PCI, HIPAA y SOX para las auditorías de cumplimiento de la normativa de seguridad vigente.
Analytics	
Prestación	Descripción
Agregación de datos	El motor de análisis basado en inteligencia automatiza la agregación, normalización, correlación y contextualización de los datos de seguridad que circulan por todos los firewalls.
Contextualización de datos	Los análisis accionables presentados de forma estructurada, significativa y de fácil acceso permiten a los equipos de seguridad, analistas e interesados descubrir, interpretar, dar prioridad, tomar decisiones y tomar medidas defensivas adecuadas.
Análisis de flujos	Los flujos de datos de seguridad de red son procesados, correlacionados y analizados continuamente en tiempo real y los resultados se muestran en un dashboard visual dinámico e interactivo.
Análisis de usuarios	Análisis profundo de las tendencias de uso para conseguir una visibilidad total del uso, el acceso y las conexiones en toda la red.
Visualización dinámica en tiempo real	Mediante una única consola, el equipo de seguridad puede llevar a cabo análisis forenses y de investigación profundos y detallados de los datos de seguridad con una mayor precisión, claridad y velocidad.
Rápida detección y eliminación	Tecnología de investigación para perseguir actividades peligrosas y para gestionar y remediar riesgos rápidamente.
Análisis e informes de flujos	Proporciona un agente de informes de flujos para el análisis del tráfico de las aplicaciones y datos sobre el uso mediante protocolos IPFIX o NetFlow para ofrecer una supervisión en tiempo real e histórica. Ofrece a los administradores una interfaz efectiva y eficiente para supervisar visualmente su red en tiempo real. De esta forma, se 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. • Un visor en tiempo real personalizable mediante funciones de arrastrar y soltar. • 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 cinco 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.
Análisis del tráfico de aplicaciones	Ofrece a las organizaciones una visión transparente del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, así como potentes prestaciones de análisis forenses y resolución de problemas.

Visión de conjunto de las prestaciones

Dashboard resumido con visualizaciones y diagramas

- Velocidad del ancho de banda
- Uso de la CPU
- Cantidad de conexiones
- Tasa de conexión por segundo
- Índice de riesgo (escala 1-10)
- Porcentaje de bloqueos
- Total de conexiones
- Total de datos transferidos
- Principales aplicaciones
- Principales intrusiones
- Principales categorías de URL
- Principales virus
- Cantidad de virus, intrusiones, spyware, botnets

Emisión de supervisión en vivo con gráficos de barras/áreas

- Aplicaciones
- Interfaz con banda entrante/saliente, promedio, mínimo, máximo
  - Ancho de banda
  - Velocidad de paquetes
  - Tamaño de paquetes
  - Tasa de conexión
- Uso
  - Cantidad de conexiones
  - Supervisión multinúcleo

Principales dashboards resumidos con desgloses

- Aplicaciones
- Usuarios
- Virus
- Intrusiones
- Spyware
- Categorías web
- Orígenes
- Destinos
- Ubicaciones de origen
- Ubicaciones de destino
- Colas BW
- BotNet

Informes con desgloses, exportación a pdf/csv y envío programado de correos electrónicos

- Aplicaciones/Usuarios/Orígenes/Destinos
  - Conexiones
  - Total de conexiones bloqueadas
  - Conexiones bloqueadas por reglas de acceso
  - Conexiones bloqueadas por amenazas
  - Conexiones bloqueadas por filtros botnet
  - Conexiones bloqueadas por filtros GeoIP
  - Conexiones bloqueadas por Servicio de filtrado de contenido
  - Virus
  - Intrusiones
  - Spyware
  - Total de datos transferidos
  - Datos enviados
  - Datos recibidos
- Virus/Intrusiones/Spyware/Categorías web/Ubicaciones de origen/Ubicaciones de destino/Colas BW
  - Conexiones
  - Total de datos transferidos
  - Datos enviados
  - Datos recibidos
- BotNet
  - Conexiones
- Exportación
  - .pdf
  - .csv
- Informes programados
  - Informes de flujos
  - Capture Threat Assessment (SWARM)
  - Diario/Semanal/Mensual
  - Archivo/Correo electrónico/PDF

Visor de sesiones de Analytics con desgloses, filtrado, exportación de datos de sesiones individuales

- Análisis del tráfico en cualquier combinación de lo siguiente:
  - Aplicación
  - Categoría de aplicación
  - Riesgo de la aplicación
  - Firma
  - Acción
  - IP del iniciador/contestador
  - País del iniciador/contestador
  - Puerto del iniciador/contestador
  - Bytes del iniciador/contestador
  - Interfaz del iniciador/contestador
  - Índice del iniciador/contestador
  - Puerta de enlace del iniciador/contestador
  - MAC del iniciador/contestador
  - Protocolo
  - Velocidad (kbps)
  - ID del flujo
  - Intrusión
  - Virus
  - Spyware
  - BotNet
- Análisis de amenazas/bloqueos en cualquier combinación de:
  - Nombre de amenaza
  - Tipo de amenaza
  - ID de amenaza
  - Aplicación
  - Categoría de aplicación
  - Riesgo de la aplicación
  - Firma
  - Acción
  - IP del iniciador/contestador
  - País del iniciador/contestador
  - Puerto del iniciador/contestador
  - Bytes del iniciador/contestador
  - Interfaz del iniciador/contestador
  - Índice del iniciador/contestador
  - Puerta de enlace del iniciador/contestador
  - MAC del iniciador/contestador
  - Protocolo
  - Velocidad (kbps)
  - ID del flujo
  - Intrusión
  - Virus
  - Spyware
  - BotNet

Análisis de URL/bloqueos en cualquier combinación de lo siguiente:

- URL
- Categoría de URL
- Dominio de la URL
- Aplicación
- Categoría de aplicación
- Riesgo de la aplicación
- Firma
- Acción
- IP del iniciador/contestador
- País del iniciador/contestador
- Puerto del iniciador/contestador
- Bytes del iniciador/contestador
- Interfaz del iniciador/contestador
- Índice del iniciador/contestador
- Puerta de enlace del iniciador/contestador
- MAC del iniciador/contestador
- Protocolo
  - Velocidad (kbps)
  - ID del flujo
  - Intrusión
  - Virus
  - Spyware
  - BotNet

Flow Monitor de Analytics: desglose y dinamización de parámetros de flujo

- Aplicaciones
  - Nombres
  - Categorías
  - Firmas
- Usuarios
  - Nombre
  - Dirección IP
  - Nombres de dominios
  - Tipos de autenticación
- Actividades web
  - Sitios web
  - Categorías web
  - URL
- Orígenes
  - Direcciones IP
  - Interfaces
  - Países
- Destinos
  - Direcciones IP
  - Interfaces
  - Países
- Amenazas
  - Intrusiones
  - Virus
  - Spyware
  - Spam
  - BotNets
- VoIP
  - Tipos de elementos multimedia
  - ID de los llamantes
- Dispositivos
  - Direcciones IP
  - Interfaces
  - Nombres
- Contenido
  - Direcciones de correo electrónico
  - Tipos de archivos
- Gestión del ancho de banda
  - Entrante
  - Saliente
  - Todo
  - URL
  - Sesiones
  - Total de paquetes
  - Total de bytes
  - Amenazas

Star Graphs: visualizaciones punto a punto, desgloses y dinamización

- Orígenes/Usuarios/Ubicaciones/Dispositivos
  - Para/De
    - Destinos
    - Aplicaciones
    - Actividades web
    - Amenazas
  - Filtrado por
    - Cantidad de conexiones
    - Datos transferidos
    - Paquetes intercambiados
    - Cantidad de amenazas
  - Resaltado con halo para
    - Amenazas
    - Datos > 1 MB
    - Conexiones > 1000
    - Paquetes > 1000

Concesión de licencias y empaquetado

Centro de seguridad de Capture (CSC)		Tipo de licencia			
		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Requisitos para la licencia	Disponible para clientes con una suscripción activa AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Gestión	Una única consola	✓	✓	✓	
	Backup/Restauración	✓	✓	✓	
	Programación de tareas		✓	✓	
	Gestión de firewalls grupal		✓	✓	
	Herencia/Herencia inversa		✓	✓	
	Sin necesidad de intervención		✓	✓	
	Descargas de definiciones de firewall sin conexión		✓	✓	
	Flujo de trabajo		✓	✓	
Informes	Supervisión en vivo, Dashboards resumidos			✓	
	Descarga de informes: Aplicaciones, Amenazas, CFS, Usuarios, Tráfico, etc.			✓	
	Elaboración de informes programados			✓	
Análisis	Analytics (30 días de retención)				✓
	Cloud App Security (30 días de retención)				✓

Capture Security Center Información de pedido

Producto	SKU
SonicWall Capture Security Center Gestión para series TZ, NSv 10 a 100 1 año	01-SSC-3664
SonicWall Capture Security Center Gestión para series TZ, NSv 10 a 100 2 años	01-SSC-9151
SonicWall Capture Security Center Gestión para series TZ, NSv 10 a 100 3 años	01-SSC-9152
SonicWall Capture Security Center Gestión para NSA 2600 a 6650 y NSv 200 a 400 1 año	01-SSC-3665
SonicWall Capture Security Center Gestión para NSA 2600 a 6650 y NSv 200 a 400 2 años	01-SSC-9214
SonicWall Capture Security Center Gestión para NSA 2600 a 6650 y NSv 200 a 400 3 años	01-SSC-9215
SonicWall Capture Security Center Gestión e informes para series TZ, NSv 10 a 100 1 año	01-SSC-3435
SonicWall Capture Security Center Gestión e informes para series TZ, NSv 10 a 100 2 años	01-SSC-9148
SonicWall Capture Security Center Gestión e informes para series TZ, NSv 10 a 100 3 años	01-SSC-9149
SonicWall Capture Security Center Gestión e informes para NSA 2600 a 6650 y NSv 200 a 400 1 año	01-SSC-3879
SonicWall Capture Security Center Gestión e informes para NSA 2600 a 6650 y NSv 200 a 400 2 años	01-SSC-9154
SonicWall Capture Security Center Gestión e informes para NSA 2600 a 6650 y NSv 200 a 400 3 años	01-SSC-9202
SonicWall Capture Security Center Análisis para series TZ, NSv 10 a 100 1 año	02-SSC-0171
SonicWall Capture Security Center Análisis para NSA 2600 a 6650 y NSv 200 a 400 1 año	02-SSC-0391

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)

Dispositivos SonicWall compatibles gestionados por Capture Security Center

- Dispositivos SonicWall de seguridad de red: Dispositivos de las series NS*a* 2600 a NS*a* 6650 y TZ
- Dispositivos virtuales de seguridad de red de SonicWall: NSv 10 a NSv 400

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

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

Datasheet- Análisis-US-VG-MKTG4305

SONICWALL®