SONICWALL

Capture Security appliance 1000 de SonicWall

El dispositivo Capture Security Appliance™ (CSa) de SonicWall incorpora Capture Advanced Threat Protection™ (ATP) y *sandboxing* para el análisis de *malware* a escenarios de implementación locales para clientes con restricciones de políticas y cumplimiento que impiden enviar archivos a la nube para su análisis, o que prefieren que todos sus datos permanezcan dentro de su organización. CSa 1000 puede analizar archivos sospechosos procedentes de otros productos de SonicWall para proporcionar rapidez y gran precisión de detección de amenazas nunca vistas con anterioridad y, a su vez, permitir que el cliente mantenga la custodia de sus archivos. Además, la funcionalidad API REST de CSa aporta los beneficios de esta capacidad de análisis de archivos altamente efectiva a los equipos de inteligencia de amenazas, los sistemas de seguridad de terceros y a cualquier pila de software que pueda integrarse con las API publicadas.

El dispositivo CSa utiliza una combinación de controles basados en la reputación, el análisis estático de archivos y el motor patentado Real-Time Deep Memory Inspection™ (RTDMI, Inspección de memoria profunda en tiempo real) de SonicWall para el análisis dinámico con el fin de garantizar que no solo ofrece la mejor tasa de detección posible de archivos maliciosos, sino que también lo hace de manera eficiente y en el menor tiempo posible. El ecosistema de productos de seguridad de SonicWall, que ya está totalmente integrado con el análisis Capture ATP en la nube, es capaz de reforzar la seguridad interna con funciones como la de Bloqueo hasta que haya un veredicto.

Estas capacidades son también compatibles cuando los productos de SonicWall se conectan a la serie CSa en lugar de a Capture ATP en la nube.

RTDMI

El motor de análisis de archivos Real-Time Deep Memory Inspection (RTDMI, Inspección de memoria profunda en tiempo real) de SonicWall, pendiente de patente, es un método novedoso para analizar archivos sospechosos mediante la supervisión del comportamiento de una aplicación en la memoria. RTDMI permite identificar cualquier técnica de confusión o cifrado que el software malicioso moderno pueda desplegar para evadir el análisis de red y de *sandbox*, lo que produce una detección sumamente precisa de los ataques incluidos en documentos, ejecutables, ficheros de almacenamiento y otros tipos de archivos.

Prevención en tiempo real

La combinación de controles de reputación e inteligencia global, análisis estáticos y tecnología RTDMI funciona en conjunto para ofrecer resultados lo suficientemente rápidos como para permitir tecnologías como la de Bloqueo hasta que haya un veredicto en los productos de SonicWall. Esta capacidad permite una política de inspección de archivos en el firewall para evitar que el usuario final descargue archivos sospechosos hasta que se haya realizado la inspección completa y se alcance un veredicto mediante Capture ATP o CSa.

Ventajas:

- Inspección basada en memoria con RTDMI
- Análisis multifase con comprobación de reputación, análisis estático y dinámico
- Acceso a API para análisis de amenazas
- Admite gran variedad de tipos de archivos
- Admite la función Bloqueo hasta que haya un veredicto
- Eficacia de alta seguridad
- Informes y acceso basado en funciones

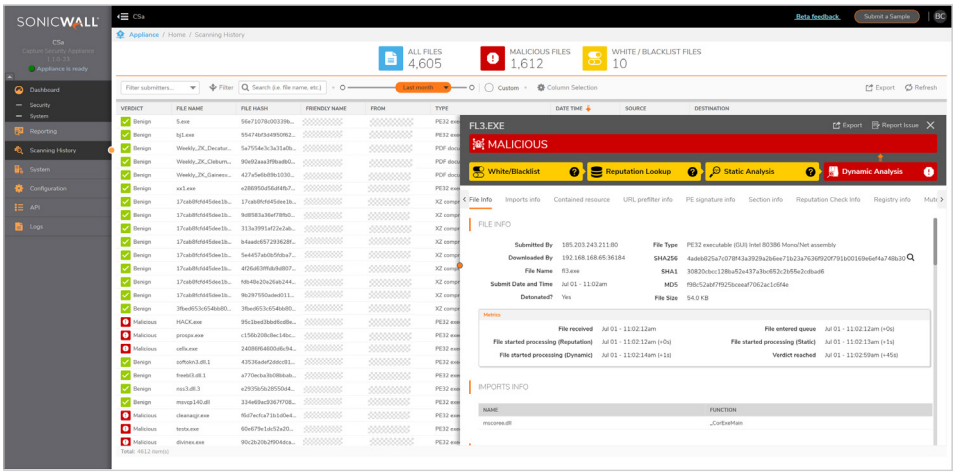
1. *El rendimiento del análisis depende de la conectividad de red, los tipos de archivos o los niveles de compresión y puede variar con respecto a las cifras publicadas.*
2. *Si bien no existe un límite estricto, el número de dispositivos se determinará en función del número de archivos enviados por cada dispositivo. El rango recomendado en la fecha de publicación es de unos 250 dispositivos.*
3. *Todas las series TZ, NSa y SuperMassive que pueden ejecutar SonicOS 6.5.4.6 o superior. No es compatible con las series SuperMassive 9800 y NSsp 12000.*

Aprovechamiento y confianza en la experiencia de muchos

- CSa combina la tecnología Capture ATP de SonicWall, un servicio basado en la nube de confianza y utilizado por más de 150 000 clientes en todo el mundo, en un factor de forma de dispositivo.
- CSa también recibe actualizaciones periódicas de inteligencia para sincronizarse con la inteligencia de amenazas recopilada a nivel global a través del análisis de archivos de Capture ATP de SonicWall.

Informes, análisis y gestión

- CSa aporta información de los archivos enviados desde todas las fuentes con un panel de control y un historial de análisis de archivos de fácil navegación, con información sobre la frecuencia, las fuentes, los veredictos y otros datos sobre los archivos enviados para ser analizados.
- Las funciones de generación de informes proporcionan una visión global de la protección ATP en toda la organización, con la posibilidad de programar informes periódicos configurados según diferentes funciones.
- Los administradores pueden otorgar acceso granular al CSa 1000 con distintas funciones y tener la posibilidad de restringir el acceso a cualquier parte de la interfaz de usuario.
- Los analistas de seguridad pueden tener acceso al historial de análisis con la posibilidad de modificar la lista blanca o negra, los dispositivos permitidos e informar de cualquier sospecha de falsos positivos o negativos.
- Los administradores de red pueden tener acceso a la configuración operativa del dispositivo, pero, por motivos de confidencialidad, tener prohibido ver los archivos enviados y sus fuentes.



Prestaciones

- Búsqueda de reputación y veredicto global (configurable)
- Análisis estático y dinámico con RTDMI
- Lista blanca o negra en base al *hash* o el dominio
- Informes programados configurables
- Gestión basada en funciones (funciones configurables)
- Gestión: HTTPS o SSH a través de una interfaz de gestión específica o una interfaz de red convencional
- Acceso a la consola SSH
- Registro y alertas
- Notificación de falsos positivos y negativos con generación automática de lista blanca o negra
- Conectividad directa o a través de VPN (IP direccionable)
- Funcionamiento en red cerrada
- Compatibilidad con API REST para presentación y análisis de archivos
- Sistema operativo reforzado con arranque seguro y cadena de confianza para antimanipulación
- Registro local

1. *El rendimiento del análisis depende de la conectividad de red, los tipos de archivos o los niveles de compresión y puede variar con respecto a las cifras publicadas.*
2. *Si bien no existe un límite estricto, el número de dispositivos se determinará en función del número de archivos enviados por cada dispositivo. El rango recomendado en la fecha de publicación es de unos 250 dispositivos.*
3. *Todas las series TZ, NSa y SuperMassive que pueden ejecutar SonicOS 6.5.4.6 o superior. No es compatible con las series SuperMassive 9800 y NSsp 12000.*

Opciones de implementación

- La implementación del dispositivo CSa de SonicWall es rápida y sencilla y, para empezar, requiere configurar la red básica, los informes y el acceso de dispositivos permitidos.
- CSa está diseñado para ser direccionable por IP y, por lo tanto, puede implementarse en cualquier lugar siempre que sea accesible por los dispositivos que enviarán archivos para ser analizados.

Existen tres métodos principales de implementación para CSa 1000:

Oficina única o ubicación única

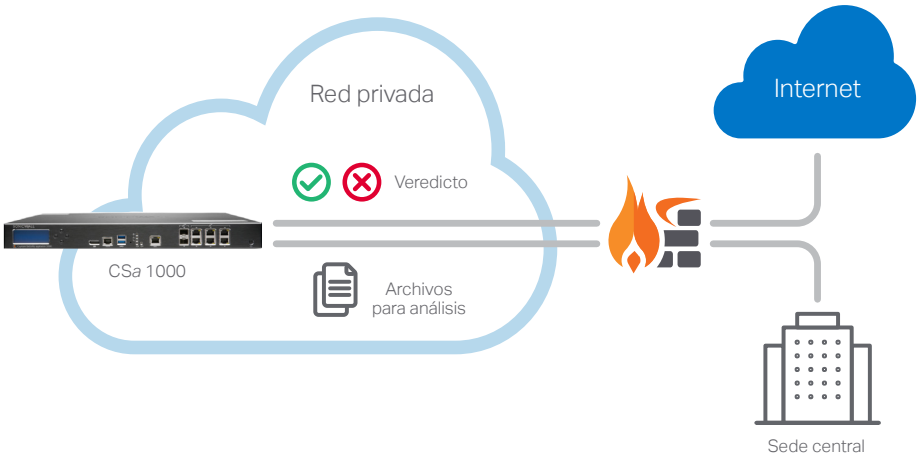
- CSa puede instalarse en cualquier lugar de la red siempre que los productos que lo utilicen puedan acceder al mismo a través de una IP.[1]
- Una vez implementado el dispositivo CSa, los firewalls y sistemas de la solución Email Security (otras soluciones pendientes) pueden configurarse para redirigir los archivos sospechosos al CSa en lugar de a la nube para el análisis de ATP.

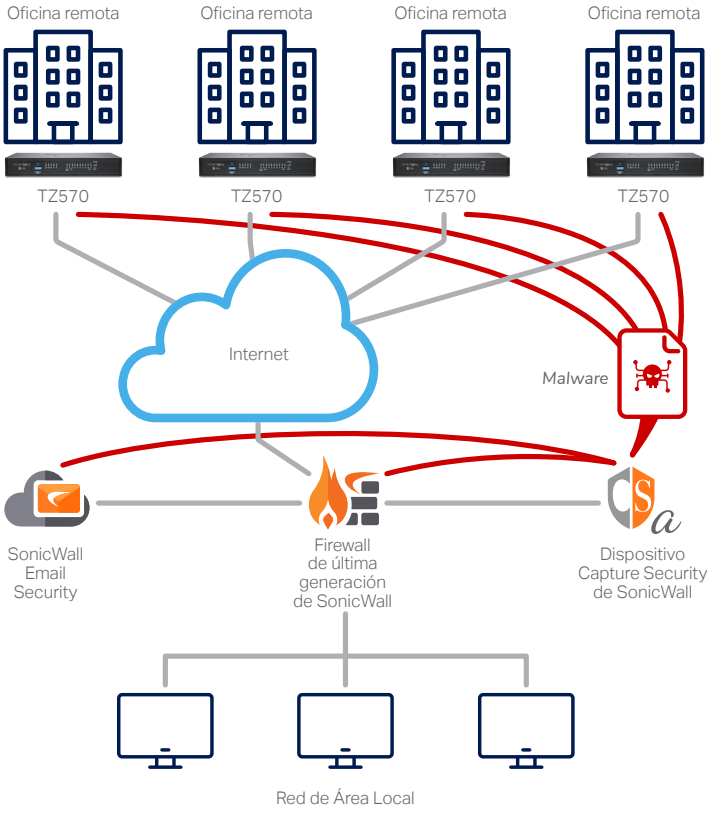
Empresa distribuida o múltiples ubicaciones

- Se pueden configurar varias oficinas u oficinas remotas para compartir el acceso a un único dispositivo CSa, instalado bien en el centro de datos de la sede central o bien en un centro de datos remoto al que pueden acceder todos los dispositivos.
- El acceso puede ser directo a través de Internet o a través de una VPN.
- La configuración masiva de los sistemas de SonicWall para dirigirse al CSa se puede hacer con GMS o con las soluciones de gestión centralizada NSM basadas en la nube para una configuración e implantación rápidas.

Gateway API REST

- La serie CSa tiene una interfaz API REST que puede utilizarse para que los equipos de inteligencia contra amenazas envíen archivos para su análisis y los resultados de las consultas a través de sus propios *scripts*, integraciones de portal web y otros productos de seguridad.
- Puede encontrar instrucciones sobre cómo comenzar con la creación de *scripts* para API para el dispositivo CSa y muestras de código en https://github.com/sonicwall

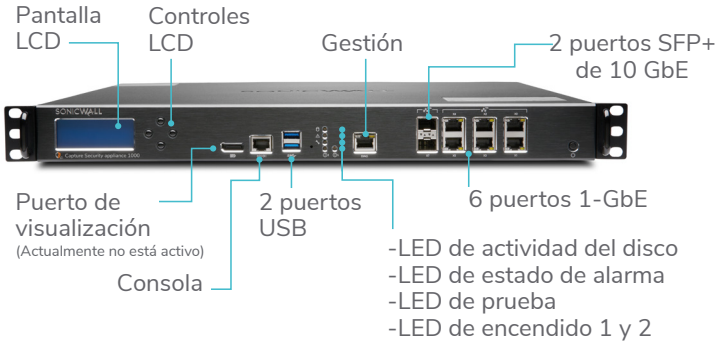




* [1]*Los firewalls de SonicWall también requieren acceso a través de UDP por el puerto 2259.*

1. *El rendimiento del análisis depende de la conectividad de red, los tipos de archivos o los niveles de compresión y puede variar con respecto a las cifras publicadas.*
2. *Si bien no existe un límite estricto, el número de dispositivos se determinará en función del número de archivos enviados por cada dispositivo. El rango recomendado en la fecha de publicación es de unos 250 dispositivos.*
3. *Todas las series TZ, NSa y SuperMassive que pueden ejecutar SonicOS 6.5.4.6 o superior. No es compatible con las series SuperMassive 9800 y NSsp 12000.*

CSa 1000



Especificaciones de CSa 1000 de SonicWall

PRESTACIONES	
Rendimiento de la búsqueda de reputación y amenazas globales (archivos por hora)[1]	12 000
Rendimiento de la combinación de archivos del mundo real (archivos por hora)[1]	2500
Rendimiento del análisis dinámico (RTDMI) (archivos por hora)[1]	300
Tamaño máximo del archivo	100 MB
Número máximo de dispositivos soportados[2]	Basado en el rendimiento
Profundidad máxima del análisis de archivos	3
Soporte API REST	Sí
Dispositivos SonicWall soportados	TZ, NSa y SuperMassive (con SonicOS 6.5.4.6 y superiores)[3] Email Security 10.X Serie NSsp 15000 - Pendiente Serie NSv (7.X y superior) - Pendiente
Tipos de archivo soportados	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
Período de conservación de datos	Sin restricciones, limitado por el almacenamiento
Almacenamiento	2 SSD de 1 TB (RAID 1)
Interfaces	6 puertos de 1 GE, 2 puertos SFP+ de 10 Gb , 2 USB, 1 consola
Gestión de puertos específica	Sí (X0)
Certificaciones	FIPS 140-2 pendiente
CARACTERÍSTICAS DEL PRODUCTO	
Factor de forma	1U
Dimensiones	17,0 x 16,5 x 1,75 pulgadas (43 x 41,5 x 4,5 cm)
Peso del dispositivo	18,3 libras (8,3 kg)
Aceleración de datos de cifrado (AES-NI)	Sí
MTBF (a 25 °C o 77 °F) en horas	129.601
Alimentación	Dos fuentes de alimentación, intercambiables en caliente
Potencia de entrada	100-240 VCA, 1,79 A
Consumo de energía	114 W
Disipación de calor total	389 BTU
Entorno	WEEE, EU RoHS, China RoHS
Choque no operativo	110 g, 2 ms
Emisiones	FCC, ICES, CE, C-Tick, VCCI; MIC
Seguridad	TUV/GS, UL, CE PSB, CCC, BSMI, esquema CB
Temperatura de funcionamiento	0 °C a 40 °C (32 °F a 104 °F)
TPM	Sí

1. El rendimiento del análisis depende de la conectividad de red, los tipos de archivos o los niveles de compresión y puede variar con respecto a las cifras publicadas.
2. Si bien no existe un límite estricto, el número de dispositivos se determinará en función del número de archivos enviados por cada dispositivo. El rango recomendado en la fecha de publicación es de unos 250 dispositivos.
3. Todas las series TZ, NSa y SuperMassive que pueden ejecutar SonicOS 6.5.4.6 o superior. No es compatible con las series SuperMassive 9800 y NSsp 12000.

Producto	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 con actualizaciones de inteligencia y paquete de soporte – 1 año	02-SSC-5637
Capture Security Appliance CSA 1000 con actualizaciones de inteligencia y paquete de soporte – 3 años	02-SSC-5638
Capture Security Appliance CSA 1000 con actualizaciones de inteligencia y paquete de soporte – 5 años	02-SSC-5639

Servicios (necesarios para el funcionamiento de CSa 1000. Todos los dispositivos que envían archivos a CSa deben tener licencia de Capture ATP)	SKU
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 1 AÑO	02-SSC-4712
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 2 AÑOS	02-SSC-4713
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 3 AÑOS	02-SSC-4714
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 4 AÑOS	02-SSC-4715
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 5 AÑOS	02-SSC-4716
ACTUALIZACIONES DE INTELIGENCIA, ACTIVACIÓN Y SOPORTE PARA CSA 1000 DE SONICWALL 6 AÑOS	02-SSC-4717

Activación de API REST (Este servicio se requiere únicamente para el funcionamiento de API REST. Debe aplicarse además del servicio de actualización de inteligencia, activación y soporte)	SKU
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 1 AÑO	02-SSC-4706
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 2 AÑOS	02-SSC-4707
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 3 AÑOS	02-SSC-4708
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 4 AÑOS	02-SSC-4709
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 5 AÑOS	02-SSC-4710
ACTIVACIÓN DE API REST PARA CAPTURE APPLIANCE CSA 1000 DE SONICWALL 6 AÑOS	02-SSC-4711

1. *El rendimiento del análisis depende de la conectividad de red, los tipos de archivos o los niveles de compresión y puede variar con respecto a las cifras publicadas.*
2. *Si bien no existe un límite estricto, el número de dispositivos se determinará en función del número de archivos enviados por cada dispositivo. El rango recomendado en la fecha de publicación es de unos 250 dispositivos.*
3. *Todas las series TZ, NSa y SuperMassive que pueden ejecutar SonicOS 6.5.4.6 o superior. No es compatible con las series SuperMassive 9800 y NSsp 12000.*

Acerca de SonicWall

SonicWall ofrece Boundless Cybersecurity (Ciberseguridad sin Límites, sin Perímetro) para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 (Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-CSa-US-COG-2099