

# Capture Security Center

Sea más consciente. Una solución holística integrada para la gestión total de la seguridad.

## SONICWALL CAPTURE SECURITY CENTER ES SENCILLA

con una arquitectura real de inicio de sesión único (SSO) y de un solo panel (SPOG). Vea todo su ecosistema de seguridad con una solución de gestión escalable.

**Capture Security Center (CSC)** le ofrece todo lo que necesita para una gestión completa, accesible desde una única interfaz repleta de funciones. Abarca todo: análisis y generación de informes para la seguridad de la red, la conexión inalámbrica, el correo electrónico, los endpoints y la nube, Risk Meters y gestión de activos.

CSC es una solución SaaS que le brinda mayor agilidad con una visión de 360° de todo su ecosistema de seguridad de SonicWall. Ofrece integración funcional para mejorar la eficiencia y la elasticidad de las operaciones con una verdadera interfaz SPOG. Dé respuestas

informadas ante cualquier amenaza, con rapidez y en tiempo real, desde cualquier ubicación y cualquier dispositivo con acceso a la web, con elaboración de informes detallados y análisis potentes.

CSC respalda su estrategia de defensa cibernética más amplia porque su diseño se ajusta a los requisitos de nivel de servicio de los Centros de Operaciones de Seguridad (SOC). Permite aplicar una estrategia unificada de control de la seguridad, cumplimiento normativo y muchas otras estrategias de gestión de riesgos, todo ello desde una aplicación habilitada para la web.



Capture Security Center es una verdadera aplicación SPOG que ofrece una solución de gestión holística e integrada. Y se incluye en la mayoría de los firewalls SonicWall y servicios de la nube.

**CAPTURE SECURITY CENTER**

Gestión, informes y análisis unificados y distribuidos en la nube para la seguridad de la red, la conexión inalámbrica, los switches, los endpoints, el correo electrónico y la nube

MÁS INFORMACIÓN

Legitimación

# Obtenga mayor eficiencia y flexibilidad de las operaciones

Sea más eficaz. Trabaje más rápido y de manera más inteligente con menos esfuerzo.

## CAPTURE SECURITY CENTER ES MÁS EFICIENTE

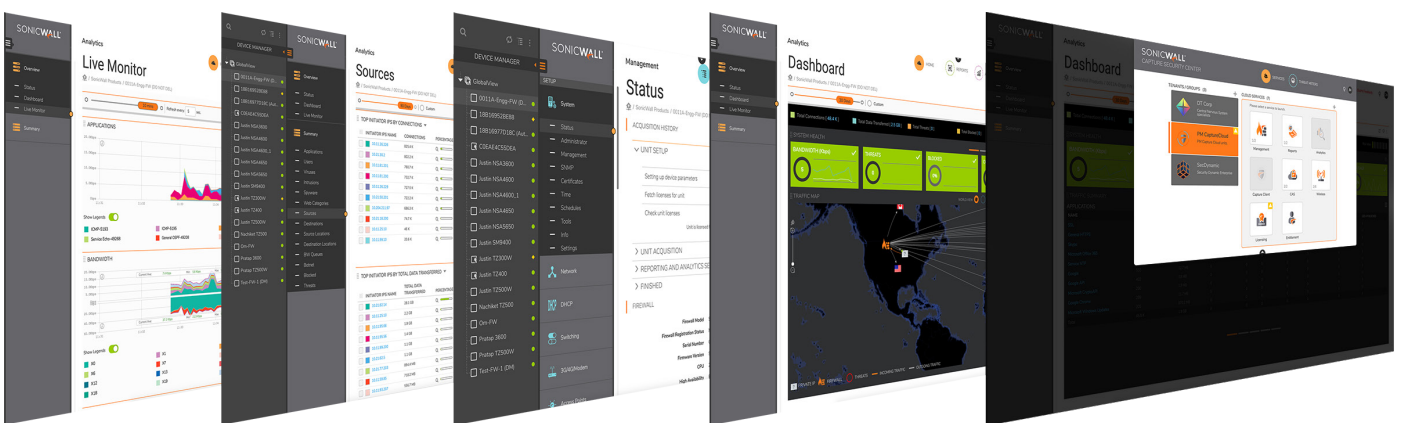
Gestione más con una solución SPOG. Abarque todo lo que tenga en su infraestructura y red de seguridad, incluida la arquitectura, las ciberamenazas y los problemas de conformidad con la normativa.

CSC es una herramienta de gestión de la productividad con escalabilidad integrada y una mejor coordinación de la administración.

SSO abre todos los aspectos operativos de la red: desde la seguridad en la nube a los endpoints. El diseño nativo de la nube le permite disponer de todo lo que necesita en un marco simple y común. Cada tarea es más sencilla y eficaz.

Reduzca el tiempo y los gastos que conllevan las tareas cotidianas. Elimine silos de seguridad innecesarios y obtenga una eficiencia que precise solo “ver y hacer clic” en todos los flujos de trabajo esenciales. Adquiera nuevas capacidades tan pronto como estén disponibles.

Gestione toda su pila de seguridad de SonicWall desde un único lugar. Identifique las brechas y los riesgos de seguridad con Risk Meters y análisis precisos. Responda antes con información crítica sobre amenazas en las que el tiempo es crucial y con conocimiento de la situación. Simplifique el flujo de trabajo de gestión, reduzca las malas configuraciones y los errores humanos y proporcione fácilmente firewalls, switches y access points remotos en las oficinas remotas utilizando la Implementación Zero-Touch (sin necesidad de intervención).



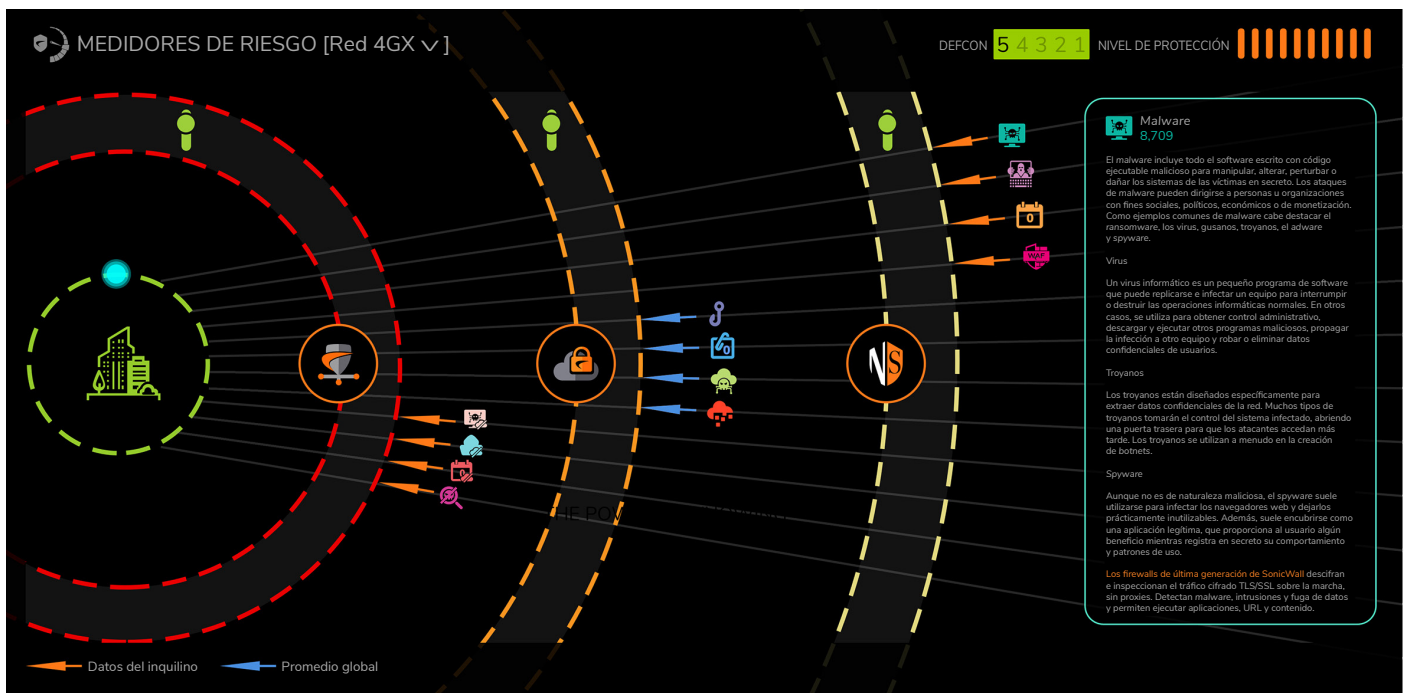
El diseño nativo de la nube aumenta la eficiencia y la elasticidad de las operaciones. Reduzca los silos de seguridad y aumente la productividad en todo el entorno de seguridad, todo ello desde una única aplicación.

# Inteligencia sincronizada sobre ciberamenazas para toda su red

Esté seguro. Estudie sus riesgos y amenazas, en tiempo real con datos del mundo real.

## CAPTURE SECURITY CENTER ACTÚA DE FORMA INTELIGENTE FRENTE A LAS AMENAZAS

Fusione datos personalizados en función del estado actual de sus activos de seguridad con la inteligencia actual sobre ciberamenazas. Defienda su red basándose en datos de riesgo reales, en tiempo real.



Los medidores de riesgo (Risk Meters) muestran automáticamente los datos sobre amenazas y las calificaciones de riesgo en función de los datos sobre amenazas reales en comparación con su nivel actual de protección. Revele brechas en las capas defensivas y tome decisiones de seguridad en tiempo real. Oriente las decisiones sobre planificación, políticas y presupuestos de seguridad en función de la puntuación lógica.

Con **SonicWall Risk Meters**, puede personalizar su evaluación de seguridad en función de los requisitos específicos de su infraestructura de red. Vea las amenazas a las que se enfrenta su red proyectadas en un análisis en tiempo real asistido por gráficos. Este recurso integrado permite a sus equipos

de seguridad ver los vectores de amenazas e identificar lo que hay que hacer para defender la red. Observe cómo las amenazas convergen en su red desde la web, la nube, las aplicaciones, los endpoints, los dispositivos móviles, las bases de datos y el Internet de las Cosas. Visualice las brechas de seguridad

potenciales, reconozca los ataques entrantes, supervise todas las fuentes posibles, incluidos los servicios de terceros, y tome medidas defensivas. Elimine los ataques imprevistos y aumente el nivel de seguridad de su red en función de lo que ocurre en tiempo real.

# Administrar la seguridad sin problemas

Asuma el control. Realice sus operaciones de seguridad desde un único lugar.

## CAPTURE SECURITY CENTER ES INTEGRIDAD

Logre mayor control visual de sus entornos de seguridad al mismo tiempo a fin de simplificar los procesos de gestión y cuentas, acelerar la toma de decisiones, mejorar el soporte y corregir las brechas de seguridad.

The screenshot displays the SonicWall My SonicWall dashboard. The interface includes a sidebar with navigation options like 'My Workspace BETA', 'Tenant Products', 'Register Products', 'User Groups', 'Overview', and 'Product Management'. The main content area shows a 'Search Tenant' field and a grid of tenant cards. Each card lists metrics for Firewalls, Access Points, EndPoints, Cloud Users, Licence Status (with a color-coded indicator), and Downloads Available. Below the tenant cards are several utility panels: 'Register products' with a diagram, 'Licensing status' showing 'Expiring Soon' (3) and 'Expired' (33) counts, 'Downloads Available' listing 'CSC-MA Documentation Maintenance Release' and 'TZ400 Beta Firmware Beta Release', 'Customer Products' showing 4 Customers and 82 Products, 'User management' showing 9 User Groups and 0 Users, and 'Support Cases' showing 0 'Waiting on Customer' and 0 'Open' cases. The footer includes the version '©SonicWall version:14.6' and a navigation bar with links like 'Quick Register', 'Report Issues', 'Downloads', 'Security Center', 'Demos', 'TOS', 'Privacy', and 'Feedback'.

Accesible desde la consola en la nube Capture Security Center, la interfaz My Workspace de My SonicWall le permite realizar sus operaciones de seguridad complejas de una forma más sencilla y eficaz. Sus flujos de trabajo sistemáticos le permiten incorporar, configurar y gestionar de forma fácil y rápida múltiples usuarios en campus, oficinas remotas o grupos funcionales, realizar el registro masivo de

productos, activar licencias y asistencia e iniciar pruebas de productos bajo demanda.

Los flujos de trabajo de usuarios proporcionan acceso instantáneo a sus equipos de operaciones de seguridad de todas las organizaciones, como el control de acceso granular basado en funciones a los productos gestionados por Capture Security Center.

Un panel de control intuitivo le ofrece visibilidad y conocimiento instantáneos de los productos que tienen licencias por vencer o de los productos que necesitan actualizaciones de software o firmware. Participe, colabore y comuníquese con los usuarios y facilite, controle y resuelva los problemas y las solicitudes de asistencia utilizando un portal de autoservicio integrado.

# Resumen de las prestaciones de CSC

## Gestión

- Acceso a la mayoría de funciones desde un único panel
- Múltiples sesiones de usuario simultáneas
- Seguridad centralizada y gestión de red
- Cuadro de mando universal
- Gestión de firewall
- Gestión de switch de SonicWall
- Gestión inalámbrica
- Configuración de políticas federadas
- Definición de políticas a nivel de grupo
- Replicación de políticas desde un dispositivo a un único dispositivo o un grupo de dispositivos
- Gestión de órdenes de cambio y flujo de trabajo
- Implementación Zero-Touch
- Configuraciones de dispositivos Zero-Touch proporcionadas previamente
- Implementación y configuración de VPN
- Supervisión y alertas de dispositivos activos
- Visualización e inteligencia de las aplicaciones
- Soporte de API, CLI y SNMP

- Gestión de Capture Client
- Gestión de Cloud App Security
- Gestión de Hosted Email Security
- MySonicWall y MyWorkspace
- Medidores de riesgos
- Centro de seguridad
- Cloud App Security - TI en la sombra
- Gestión de licencias
- Gestión basada en funciones (usuarios, grupos)
- Copia de seguridad de los archivos de preferencia del dispositivo de firewall

## Supervisión

- Supervisión y alertas de dispositivos
- Flujos de datos IPFIX en tiempo real
- Supervisión y alertas de dispositivos activos
- Gestión del relé SNMP
- Supervisión del estado de VPN y firewalls
- Medidores de riesgos

## Generación de informes

- Registro de firewall centralizado
- Informes basados en Syslog o IPFIX
- Informes PDF programados y personalizados
- Informes multiamenaza
- Informes centrados en el usuario
- Informes de uso de las aplicaciones
- Informes de botnets
- Informes de Geo IP
- Informes de direcciones MAC
- Informes de Capture ATP
- Informes de access points inalámbricos no fiables
- Informes de Cloud App Security (CAS)
- Informes de Capture Client
- Informes de ancho de banda y servicios por interfaz

## Análisis

- Actividades basadas en los usuarios
- Uso de las aplicaciones
- Visibilidad entre productos con Capture Client
- Visualización dinámica en tiempo real
- Capacidades de desglose y giro

## Licencias y paquetes

Los servicios basados en la nube están disponibles en las siguientes opciones de paquetes.

### 1. CSC Basic Management (Lite)

Esta versión es la más adecuada para la copia de seguridad y restauración del sistema o las preferencias del firewall y para la actualización del firmware. Cualquier firewall con suscripción AGSS o CGSS puede activar esta funcionalidad de gestión básica para ayudar a gestionar los firewalls.

### 2. Gestión de CSC

Esta opción de suscripción de pago activa todas las capacidades de gestión, como Workflow Automation y Implementación Zero-Touch.

### 3. Gestión e informes de CSC

Esta opción de licencia es ideal para instituciones más grandes, con muchos firewalls implementados en ubicaciones geográficamente dispersas que se encuentran bajo administración a nivel de grupo o basada en inquilinos. Entre ellas se incluyen organizaciones del mercado medio, empresas distribuidas, sector público y organizaciones educativas con muchos distritos y campus, y proveedores de servicios gestionados (MSP).

Además de todas las funciones de gestión, esta opción de suscripción ofrece funciones completas de generación de informes para realizar auditorías y revisiones periódicas o por encargo del rendimiento de la red y de la seguridad. Esto se puede hacer utilizando el cuadro de mando interactivo universal en pantalla con gráficos y tablas en vivo o fuera de pantalla con informes exportados y planificados.

### 4. CSC Analytics

Se trata de un potente servicio complementario para todas las opciones de suscripción de Capture Security Center. La activación del servicio proporciona acceso completo a las herramientas y servicios de SonicWall Analytics y SonicWall Cloud App Security para llevar a cabo investigaciones forenses de red y búsqueda de amenazas utilizando capacidades integrales de desglose y giro. CSC Analytics también incluye 30 días de almacenamiento de archivos de registro y 365 días de generación de informes.

## Modelos de firewall compatibles

Capture Security Center está disponible para clientes con firewalls de las series SOHO-W, SOHO 250, SOHO 250W, TZ, NSA, NSa 2650-6650 y NSv. Para las series SuperMassive 9000, NSa y NSp 12400 a 12800, la opción de suscripción a CSC Management se activa automáticamente como parte de su correspondiente activación de suscripción a AGSS.

### CAPTURE SECURITY CENTER

	Gestión	Generación de informes <sup>4</sup>	Análisis <sup>4</sup>
FW básico	Series SOHO-W, SOHO 250, SOHO 250W, TZ, NSv 10-100	Series SOHO-W, SOHO 250, SOHO 250W, TZ, NSv 10-100	Series SOHO-W, SOHO 250, SOHO 250W, TZ, NSv 10-100
FW de gama media	Serie NSA, serie NSa, NSv 200-400	Serie NSA, serie NSa, NSv 200-400	Serie NSA, serie NSa, NSv 200-400
FW de gama alta	Serie SuperMassive 9000, serie NSp 12000, NSa 9250-9650, NSv 800-1600	Serie SuperMassive 9000, serie NSp 12000, NSa 9250-9650, NSv 800-1600	Serie SuperMassive 9000, serie NSp 12000, NSa 9250-9650, NSv 800-1600

<sup>4</sup>La compatibilidad con generación de informes y análisis para FW de gama alta solo está disponible en On\_prem Analytics.

	Prestaciones	CSC Management Lite	Gestión de CSC	Gestión e informes de CSC	Análisis SaaS	Análisis in situ
Gestión	Copia de seguridad/restauración: sistema del firewall	Sí	Sí	Sí	Sí	Sí <sup>2</sup>
	Copia de seguridad/restauración: preferencias del firewall	Sí	Sí	Sí	Sí	Sí <sup>2</sup>
	Actualización de firmware	Solo desde archivo local	Solo desde archivo local o MySonicWall	Sí	Solo desde archivo local	Solo desde archivo local <sup>3</sup>
	Planificación de tareas	-	Sí	Sí	-	-
	Gestión de grupos de firewalls	-	Sí	Sí	-	-
	Herencia: hacia adelante/hacia atrás	-	Sí	Sí	-	-
	Implementación Zero-Touch <sup>1</sup>	-	Sí	Sí	-	-
	Descargas de firmas de firewall sin conexión	-	Sí	Sí	-	-
	Flujo de trabajo	-	Sí	Sí	-	-
	Licencias agrupadas: búsqueda, uso compartido, inventario de códigos de activación utilizados	-	Sí	Sí	-	-
Generación de informes (basado en Netflow/IPFIX)	Planificar informes, supervisión en directo, paneles de control de síntesis	-	-	Sí	Sí	Sí
	Descargar informes: aplicaciones, amenazas, CFS, usuarios, tráfico, origen/destino (informes de flujo durante 1 año)	-	-	Sí	Sí	Sí
Análisis (basada en Netflow/IPFIX)	Investigación forense de redes y búsqueda de amenazas mediante desglose y giro	-	-	-	Sí	Sí
	Cloud App Security - TI en la sombra	-	-	-	Sí	No
	Retención de datos	-	-	-	Tráfico durante 30 días	1 año
Asistencia técnica		Solo casos web	Soporte 24x7	Soporte 24x7	Soporte 24x7	Soporte 24x7

<sup>1</sup> Compatible con SOHO-W con firmware 6.5.2+; series TZ, NSA y NSa 2650-6650 con firmware 6.5.1.1+. No es compatible con las series SOHO ni NSv.

<sup>2</sup> Requiere el servicio AGSS/CGSS o cualquier servicio de pago de Capture Security Center

<sup>3</sup> Requiere una licencia de soporte 24x7

## Información sobre referencias

Producto	SKU
SonicWall Capture Security Center Management para la serie TZ, SOHO-W, SOHO 250, SOHO 250W, NSv 10 a 100 1 año	01-SSC-3664
SonicWall Capture Security Center Management para la serie TZ, SOHO-W, SOHO 250, SOHO 250W NSv 10 a 100 2 años	01-SSC-9151
SonicWall Capture Security Center Management para la serie TZ, SOHO-W, SOHO 250, SOHO 250W NSv 10 a 100 3 años	01-SSC-9152
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 1 año	01-SSC-3665
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 2 años	01-SSC-9214
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 3 años	01-SSC-9215
SonicWall Capture Security Center Management and Reporting para la serie TZ, SOHO-W, SOHO 250, SOHO250W, NSv 10 a 100 1 año	01-SSC-3435
SonicWall Capture Security Center Management and Reporting para la serie TZ, SOHO-W, SOHO 250, SOHO250W, NSv 10 a 100 2 años	01-SSC-9148
SonicWall Capture Security Center Management and Reporting para la serie TZ, SOHO-W, SOHO 250, SOHO250W, NSv 10 a 100 3 años	01-SSC-9149
SonicWall Capture Security Center Management and Reporting para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 1 año	01-SSC-3879
SonicWall Capture Security Center Management and Reporting para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 2 años	01-SSC-9154
SonicWall Capture Security Center Management and Reporting para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 3 años	01-SSC-9202
SonicWall Capture Security Center Analytics para la serie TZ, SOHO-W, SOHO 250, SOHO250W, NSv 10 a 100 1 año	02-SSC-0171
SonicWall Capture Security Center Analytics Management para NSA 2600 a 6600, NSa 2650 a 6650 y NSv 200 a 400 1 año	02-SSC-0391

### Navegadores de Internet

- Microsoft® Internet Explorer 11.0 o superior (no usar el 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 de seguridad de la red de SonicWall: SuperMassive E10000 y serie 9000, E-Class NSA, serie NSsp, serie NSa, serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Dispositivos virtuales de seguridad de red de SonicWall: serie NSv
- Seguridad de endpoints de SonicWall: Capture Client
- Seguridad de la nube de SonicWall: Cloud App Security (CAS)
- SonicWall Email Security
- Web Application Firewall de SonicWall
- Acceso móvil seguro de SonicWall: serie SMA 100

### 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](http://www.sonicwall.com).