SONICWALL

# Capture Client de SonicWall

La creciente amenaza del *ransomware* y otros ataques maliciosos de *malware* ha demostrado la imposibilidad de medir las soluciones de protección de los clientes en función exclusivamente del cumplimiento normativo de los *endpoints*. La tecnología tradicional de los antivirus adopta un enfoque basado en firmas asediado desde hace mucho tiempo e incapaz de responder a las nuevas técnicas evasivas y *malware*. Además, dada la proliferación de las opciones de teletrabajo, movilidad y BYOD (lleve su propio dispositivo), existe la urgente necesidad de ofrecer una protección constante de *endpoints* en todas partes.

SonicWall Capture Client es un *endpoint* unificado que ofrece diversas prestaciones de protección. Gracias al motor de protección contra amenazas de *malware* de nueva generación de SentinelOne, Capture Client aplica técnicas de protección avanzada ante amenazas, como el aprendizaje automático, la integración de *sandbox* en la red y la reversión de sistemas. Capture Client también utiliza la inspección profunda del tráfico cifrado mediante TLS (DPI-SSL) en los firewalls SonicWall gracias a la instalación y gestión de certificados TLS de confianza.

Capture Client coexiste con SonicWall Global VPN Client, por lo que es posible gestionar políticas para todos los productos desde una única consola de gestión basada en la nube. Capture Client puede incorporarse fácilmente a cualquier cliente implementado a través de políticas de grupo de Microsoft Active Directory, cualquier otra técnica de implementación de software de terceros; o mediante el suministro de URL personalizadas desde donde los clientes pueden descargar e instalar ellos mismos de forma silenciosa sin intervención adicional. Además, al integrarse con los firewalls de SonicWall, Capture Client permite la implementación sin necesidad de intervención en clientes desprotegidos con capacidades de cumplimiento opcionales.

## Prestaciones y ventajas

La **monitorización continua del comportamiento** del *endpoint* permite crear un perfil completo de la actividad de los archivos, las aplicaciones y los procesos, así como de la red. De este modo, se obtiene protección contra el *malware* basado y no basado en archivos y una visión de los ataques de 360 grados con información procesable pertinente para las investigaciones.

Las **múltiples técnicas multicapa basadas en la heurística** para protección comprenden información de la nube, análisis estáticos avanzados y protección dinámica de comportamientos. Estas técnicas ofrecen protección y corrección contra *malware* conocido y desconocido.

La **no necesidad de análisis y actualizaciones periódicos** ofrece el mayor nivel de protección en todo momento sin obstaculizar la productividad de los usuarios. Capture Client realiza un análisis completo durante la instalación y después realiza una supervisión continua para detectar actividades sospechosas.

La **integración de Capture Advanced Threat Protection (ATP)** carga automáticamente los archivos sospechosos para someterlos a un análisis de *sandboxing* avanzado mediante la manipulación de código que los *endpoints* no pueden realizar. Podrá detener más amenazas, como el *malware*, antes de que se ejecuten con tiempos de demora integrados.

## Ventajas

- Gestión independiente basada en la nube
- Sinergia con firewalls SonicWall
- Aplicación de las políticas de seguridad
- Gestión de certificados DPI-SSL
- Monitorización continua del comportamiento
- Determinaciones altamente precisas gracias al aprendizaje automático
- Múltiples técnicas multicapa basadas en la heurística
- Inteligencia sobre vulnerabilidades de aplicaciones
- Funcionalidades únicas de restauración
- Fácil elaboración de listas blancas y negras
- *Sandbox* en la nube Capture Advanced Threat Protection (ATP) para análisis automatizado de *malware*
- Uso compartido de información sobre amenazas sin necesidad de cargarla para la inspección manual de archivos
- Filtrado de contenido
- Control de dispositivos

Los administradores también pueden consultar la base de datos de Capture ATP sobre veredictos de archivos sin necesidad de cargarlos en la nube para analizarlos.

La **exclusiva función de reversión** también admite políticas que, además de eliminar la amenaza por completo, restauran el cliente afectado al estado en que se encontraba antes de que se iniciara la actividad de *malware*. De este modo, desaparece la necesidad de realizar restauraciones manuales si se produce algún ataque de *ransomware* o de otro tipo similar en Windows.

La **inteligencia sobre vulnerabilidades de aplicaciones** brinda a los administradores la capacidad de catalogar cada aplicación en cada *endpoint* protegido y cualquier riesgo asociado con ella. El riesgo se basa en la presencia de vulnerabilidades conocidas con detalles de las CVE y los niveles de gravedad notificados para esa versión, lo que brinda al administrador información práctica para priorizar el parcheo y reducir la superficie de ataque del *endpoint*.

La **integración opcional con los firewalls SonicWall de 6.ª generación y posteriores** ofrece implementación sin necesidad de intervención y mejora el cumplimiento normativo de los *endpoints*. Además, permite la aplicación de inspección profunda de paquetes de tráfico cifrado (DPI-SSL) mediante la implantación de certificados de confianza en cada *endpoint*.

El **filtrado de contenido** permite a las organizaciones bloquear direcciones IP y dominios de sitios maliciosos, así como aumentar la productividad del usuario al regular el ancho de banda o restringir el acceso a contenido web inaceptable o improductivo.

El **control de dispositivos** permite a las organizaciones impedir que los dispositivos potencialmente infectados se conecten al *endpoint* con políticas de listas blancas pormenorizadas.

**Gestión centralizada y generación de informes de protección de clientes** La consola de gestión basada en la nube de SonicWall funciona como un solo panel para gestionar todas las políticas de cliente: protección contra *malware* de última generación, gestión de certificados DPI-SSL y filtrado de contenido.

La consola de gestión es una plataforma multiempresa basada en la nube que se ofrece sin coste añadido. Proporciona informes de protección de clientes y gestión de políticas, con el respaldo de políticas de control de acceso pormenorizado, como la capacidad de asignar políticas basadas en atributos de Microsoft Active Directory. Esto permite a los proveedores de servicios gestionados (MSP) gestionar e informar sobre los clientes de diversos clientes. Asimismo, cada uno de estos clientes solo puede gestionar e informar sobre sus propios clientes.

La consola de gestión también funciona como una plataforma de investigación que permite identificar la causa fundamental de las amenazas detectadas de *malware* y facilita información procesable sobre cómo impedir que se repitan. Por ejemplo, un administrador puede ver fácilmente qué aplicaciones se están ejecutando en un cliente, lo cual, a su vez, ayuda a identificar los equipos que pueden estar ejecutando software vulnerable o no autorizado.

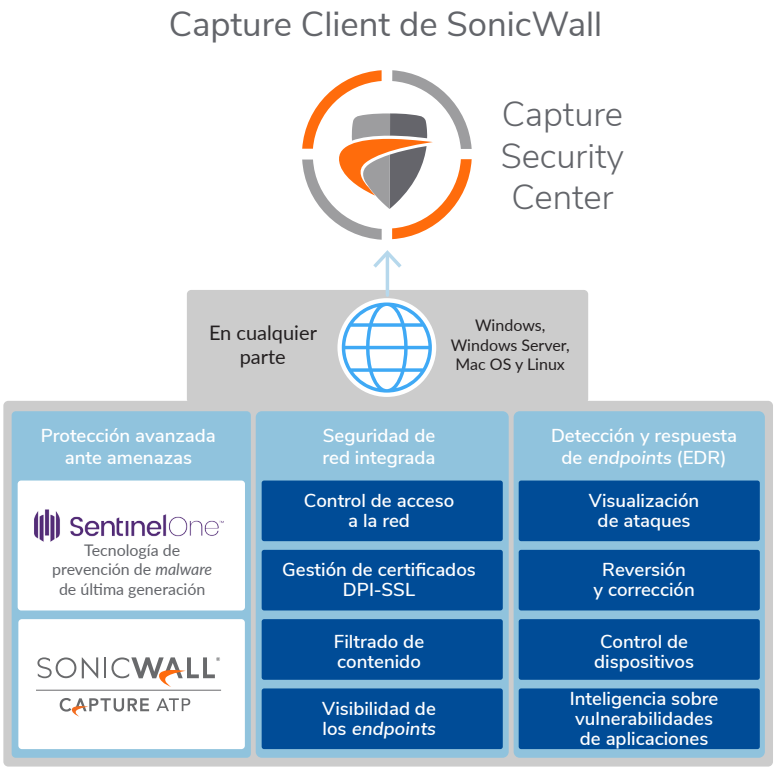
## Modalidades y compatibilidad con plataformas

Capture Client de SonicWall tiene dos modalidades:

**SonicWall Capture Client Basic** ofrece protección contra *malware* de SonicWall de última generación y características de corrección, y admite DPI-SSL.

**SonicWall Capture Client Advanced** comprende todo lo mencionado anteriormente para la modalidad Basic, además de funciones de reversión avanzadas, integración con Capture ATP, visualización de ataques, inteligencia sobre vulnerabilidades de aplicaciones y filtrado de contenido.

Ambas modalidades están disponibles para Windows 7 y posteriores, así como para Mac OSX.



| COMPARACIÓN DE PRESTACIONES | | |
|---|---|---|
| **Función** | **Basic** | **Advanced** |
| Gestión, elaboración de informes y análisis en la nube (CSC) | ✓ | ✓ |
| **Seguridad de red integrada** | | |
| Visibilidad de los *endpoints* | ✓ | ✓ |
| Implantación de certificados DPI-SSL | ✓ | ✓ |
| Filtrado de contenido | – | ✓ |
| **Protección avanzada ante amenazas** | | |
| ***Antimalware* de última generación** | ✓ | ✓ |
| Capture Advanced Threat Protection Sandboxing | – | ✓ |
| **Detección y respuesta de *endpoints*** | | |
| Visualización de ataques | – | ✓ |
| Reversión y corrección | – | ✓ |
| Control de dispositivos | – | ✓ |
| Vulnerabilidad e inteligencia de aplicaciones | – | ✓ |

| REQUISITOS DEL SISTEMA |
|---|
| **Sistemas operativos** |
| Windows 7 y posteriores |
| Windows Server 2008 R2 y posteriores |
| Mac OS/OSX 10.10 y posteriores |
| **Hardware** |
| CPU doble núcleo de 1 GHz o superior |
| 1 GB de RAM o más si lo requiere el SO (se recomiendan 2 GB) |
| 2 GB de espacio de disco disponible |

| SKU DE CAPTURE CLIENT | | |
|---|---|---|
| Producto | Validez | SKU |
| **ADVANCED** | | |
| SONICWALL CAPTURE CLIENT ADVANCED 5-24 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1518 |
| SONICWALL CAPTURE CLIENT ADVANCED 5-24 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1519 |
| SONICWALL CAPTURE CLIENT ADVANCED 25-49 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1520 |
| SONICWALL CAPTURE CLIENT ADVANCED 25-49 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1521 |
| SONICWALL CAPTURE CLIENT ADVANCED 50-99 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1522 |
| SONICWALL CAPTURE CLIENT ADVANCED 50-99 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1523 |
| SONICWALL CAPTURE CLIENT ADVANCED 100-249 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1524 |
| SONICWALL CAPTURE CLIENT ADVANCED 100-249 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1525 |
| SONICWALL CAPTURE CLIENT ADVANCED 250-499 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1454 |
| SONICWALL CAPTURE CLIENT ADVANCED 250-499 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1455 |
| SONICWALL CAPTURE CLIENT ADVANCED 500-999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1456 |
| SONICWALL CAPTURE CLIENT ADVANCED 500-999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1457 |
| SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1458 |
| SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1459 |
| SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1460 |
| SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1461 |
| SONICWALL CAPTURE CLIENT ADVANCED 10000+ *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1462 |
| SONICWALL CAPTURE CLIENT ADVANCED 10000+ *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1463 |
| BASIC | | |
| SONICWALL CAPTURE CLIENT BASIC 5-24 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1510 |
| SONICWALL CAPTURE CLIENT BASIC 5-24 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1511 |
| SONICWALL CAPTURE CLIENT BASIC 25-49 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1512 |
| SONICWALL CAPTURE CLIENT BASIC 25-49 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1513 |
| SONICWALL CAPTURE CLIENT BASIC 50-99 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1514 |
| SONICWALL CAPTURE CLIENT BASIC 50-99 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1515 |
| SONICWALL CAPTURE CLIENT BASIC 100-249 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1516 |
| SONICWALL CAPTURE CLIENT BASIC 100-249 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1517 |
| SONICWALL CAPTURE CLIENT BASIC 250-499 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1444 |
| SONICWALL CAPTURE CLIENT BASIC 250-499 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1445 |
| SONICWALL CAPTURE CLIENT BASIC 500-999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1446 |
| SONICWALL CAPTURE CLIENT BASIC 500-999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1447 |
| SONICWALL CAPTURE CLIENT BASIC 1000-4999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1448 |
| SONICWALL CAPTURE CLIENT BASIC 1000-4999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1449 |
| SONICWALL CAPTURE CLIENT BASIC 5000-9999 *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1450 |
| SONICWALL CAPTURE CLIENT BASIC 5000-9999 *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1451 |
| SONICWALL CAPTURE CLIENT BASIC 10000+ *ENDPOINTS* con asistencia 24X7 | 3 AÑOS | 02-SSC-1452 |
| SONICWALL CAPTURE CLIENT BASIC 10000+ *ENDPOINTS* con asistencia 24X7 | 1 AÑO | 02-SSC-1453 |

## Acerca de SonicWall

SonicWall ofrece ciberseguridad sin límites 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-CaptureClient-US-VG-2139