

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 o 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. Y, al integrarse con los firewalls de SonicWall, Capture Client permite la implementación silenciosa en clientes desprotegidos sin intervención alguna.

Prestaciones y ventajas

La **monitorización continua del comportamiento** del cliente 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 Advanced Threat Protection (ATP) carga automáticamente los archivos sospechosos para someterlos a un análisis 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. 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.

Ventajas

- Gestión independiente basada en web
- Sinergia con firewalls SonicWall
- Aplicación de las políticas seguridad
- Gestión de certificados DPI-SSL
- Monitorización continua del comportamiento
- Determinaciones altamente precisas gracias al aprendizaje automático
- Múltiples técnicas multicapa basadas en la heurística
- 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 inspección manual de archivos
- Protección ante amenazas web
- Control de dispositivos

La **consola de gestión basada en la nube** reduce el espacio y los gastos generales de administración. Mejora además la capacidad de implementación y aplicación de la protección de endpoints, dondequiera que estos se encuentren.

La **integración opcional con 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.

La **protección ante amenazas web y el control de dispositivos** permiten a las organizaciones bloquear sitios web y direcciones IP que se sabe que son maliciosos e impedir que dispositivos desconocidos potencialmente infectados se conecten al endpoint.

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 próxima generación, gestión de certificados DPI-SSL, filtrado de contenido y VPN.

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. Estas políticas permiten 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.

También funciona como una plataforma de investigación que permite identificar la causa fundamental de las amenazas detectadas de malware y facilitar 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.

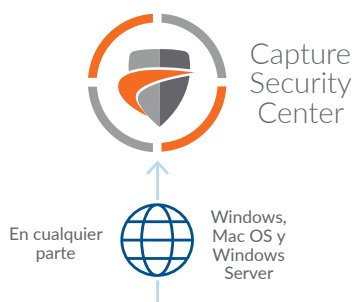
Modalidades y compatibilidad con plataformas

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 Basic, además de capacidades de reversión más opciones avanzadas, integración con Capture ATP, visualización de ataques y protección ante amenazas web.

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



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

COMPARACIÓN DE PRESTACIONES

Prestación	Capture Client Basic	Capture Client Advanced
Implantación de certificados DPI-SSL	✓	✓
Aplicación de firewall	✓	✓
Protección mediante antivirus de próxima generación (NGAV)	✓	✓
Elaboración de listas blancas y negras de aplicaciones	✓	✓
Análisis automatizado con Capture Advanced Threat Protection (ATP)	–	✓
Uso compartido de información sobre amenazas con ATP	–	✓
Remediación/Restauración	–	✓
Visualización de ataques	–	✓
Protección ante amenazas web	–	✓
Control de dispositivos	–	✓

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 lleva más de 27 años combatiendo el crimen cibernético y defendiendo a pequeñas y medianas empresas, así como a grandes compañías y agencias gubernamentales de todo el mundo. Con el respaldo de SonicWall Capture Labs, nuestras galardonadas soluciones de detección y prevención de violaciones de seguridad en tiempo real protegen más de un millón de redes, sus correos electrónicos, aplicaciones y datos, en más de 215 países y territorios. Estas organizaciones funcionan con mayor eficacia y menos temor a la seguridad. Si desea más información, visite www.sonicwall.com o síganos en [Twitter](#), [LinkedIn](#), [Facebook](#) e [Instagram](#).