

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 constante protección y aplicación de políticas web para los 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 multimotor 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.

Gestión centralizada y generación de informes de protección de clientes

La consola de gestión basada en la nube y el panel de control global de SonicWall han sido diseñados para ofrecer a los MSSP una visión global del estado de sus clientes. Los administradores pueden ver el estado de cada cliente en función del número de infecciones, las vulnerabilidades presentes, la versión de Capture Client instalada y qué y quién está siendo más bloqueado por el filtrado de contenido. Este panel de control también puede indicarle qué dispositivos están en línea y en funcionamiento.

La Política global permite a los administradores aplicar una única política de referencia a todos los clientes, lo que facilita la activación de nuevos clientes. Esto también permite a los MSSP crear rápidamente protecciones para nuevas amenazas en todos los clientes en base a esta política. Cuando se activa la opción Herencia, todos los clientes nuevos adquirirán la Política global. Cuando se desactiva, se pueden crear y modificar políticas exclusivas de clientes individuales para todo, desde el filtrado de contenido hasta la protección contra el malware y la gestión de certificados DPI-SSL.

Permite políticas de control de acceso pormenorizado, como la capacidad de asignar políticas basadas en atributos de Microsoft Active Directory, por ejemplo, por grupo de usuarios. Esto permite a los proveedores de servicios gestionados (MSSP/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.

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
- Panel de control del estado global de todos los clientes
- Fácil creación de políticas globales
- Fácil elaboración de listas de permitidos/denegados
- 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

Prestaciones y ventajas

Monitorización continua del comportamiento

- Consulte perfiles completos de actividad de archivos, aplicaciones, procesos y redes
- Protección frente al malware basado en archivos y sin archivos
- Visión de los ataques de 360 grados con información procesable

Múltiples técnicas multicapa basadas en la heurística

- Beneficiarse de la información de la nube, los análisis estáticos avanzados y la protección dinámica de comportamientos
- Protéjase y corrija el malware conocido y desconocido antes, durante o después de un ataque

No es necesario realizar análisis ni actualizaciones periódicos

- Habilite el máximo nivel de protección en todo momento sin obstaculizar la productividad de los usuarios
- Ofrece un análisis completo durante la instalación y después realiza una supervisión continua para detectar actividades sospechosas

Integración con Capture Advanced Threat Protection (ATP) (para dispositivos Windows)

- Cargue automáticamente los archivos sospechosos en dispositivos Windows para someterlos a un análisis de sandboxing avanzado
- Detecte las amenazas latentes, como el malware, antes de que se ejecuten con tiempos de demora integrados
- Consulte la base de datos de Capture ATP sobre veredictos de archivos sin necesidad de cargarlos en la nube

Funciones exclusivas de reversión (para Windows)

- Admite políticas que eliminan las amenazas por completo
- Restauración de los endpoints al estado en que se encontraban antes de que se iniciara la actividad maliciosa
- Elimine la necesidad de realizar restauraciones manuales si se produce algún ataque de ransomware o ataques similares

Inteligencia sobre vulnerabilidades de aplicaciones (para Windows y MacOS)

- Catalogue todas las aplicaciones instaladas y los riesgos asociados
- Examine las vulnerabilidades conocidas con detalles de las CVE y los niveles de gravedad notificados
- Utilice estos datos para priorizar la aplicación de parches y reducir la superficie de ataque

Integración opcional con los firewalls de SonicWall

- Permite la aplicación de inspección profunda de paquetes de tráfico cifrado (DPI-SSL) en los endpoints.
- Implante fácilmente certificados de confianza en cada endpoint.
- Dirija a los usuarios no protegidos a una página de descarga de Capture Client antes de acceder a Internet cuando estén detrás de un firewall

Filtrado de contenido (para Windows y MacOS)

- Bloqueo de direcciones IP y dominios de sitios maliciosos
- Aumento de la productividad de los usuarios al regular el ancho de banda o restringir el acceso a contenido web inaceptable o improductivo

Control de dispositivos (para Windows y MacOS)

- Impida que los dispositivos potencialmente infectados se conecten a los endpoints
- Aplique políticas de listas de permitidos pormenorizadas

Modalidades y compatibilidad con plataformas

Capture Client de SonicWall tiene dos modalidades:

SonicWall Capture Client Basic ofrece:

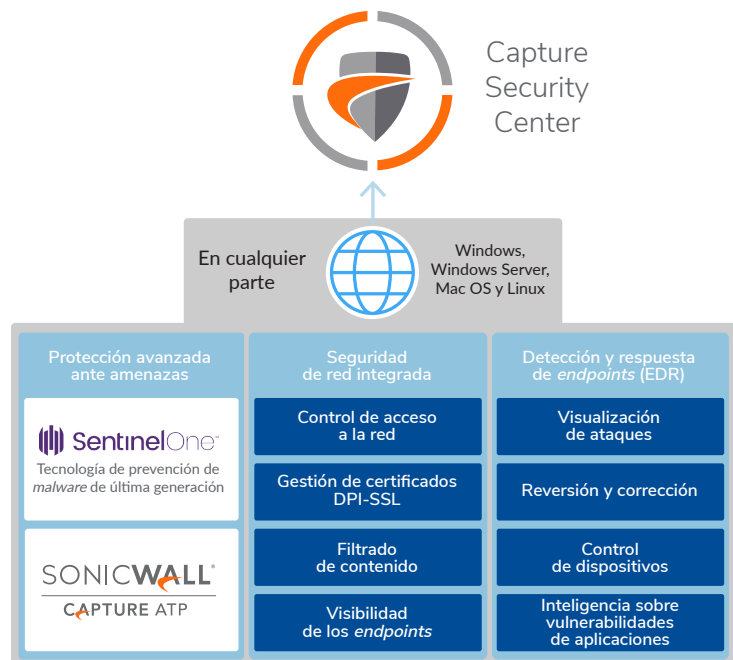
- Toda la protección contra malware de próxima generación de SonicWall
- Funciones de corrección
- Compatibilidad con DPI-SSL

SonicWall Capture Client Advanced ofrece:

- Todo lo mencionado anteriormente para la modalidad Basic
- Funcionalidades avanzadas de restauración
- Integración con Capture ATP
- Visualización de ataques
- Inteligencia sobre vulnerabilidades de aplicaciones
- Filtrado de contenido

Ambas ofertas están disponibles para Windows 7 y superior, Mac OSX y Linux (consulte a continuación los Requisitos del sistema para obtener más información).

Capture Client de SonicWall



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

AMI de Amazon Linux

Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+

Ubuntu 12.04, 14.04, 16.04, 16.10

CentOS 6.5+, 7.0+

Oracle Linux OL (anteriormente conocido como Oracle Enterprise Linux u OEL) v6.5-6.9 y v7.0+

SUSE Linux Enterprise Server 12

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, 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.