SonicWall Capture Client

Detiene las filtraciones más rápido que cualquier otra solución... de forma autónoma

La creciente amenaza del ransomware y de los demás ataques maliciosos basados en malware ha demostrado que las soluciones de protección de clientes no pueden medirse únicamente por el cumplimiento normativo de los endpoints. La tecnología antivirus tradicional utiliza un enfoque basado en definiciones que lleva tiempo causando problemas, ya que no ha sido capaz de seguir el ritmo del malware emergente ni de las técnicas de evasión.

Además, con la proliferación del teletrabajo, la movilidad y las iniciativas BYOD, surge la acuciante necesidad de proporcionar protección coherente, inteligencia de las vulnerabilidades de las aplicaciones, refuerzo de políticas Web, etc. para los endpoints allá donde se encuentren. SonicWall Capture Client es una solución unificada para endpoints con múltiples prestaciones de Protección de endpoints (EPP) y Detección y respuesta para endpoints (EDR).

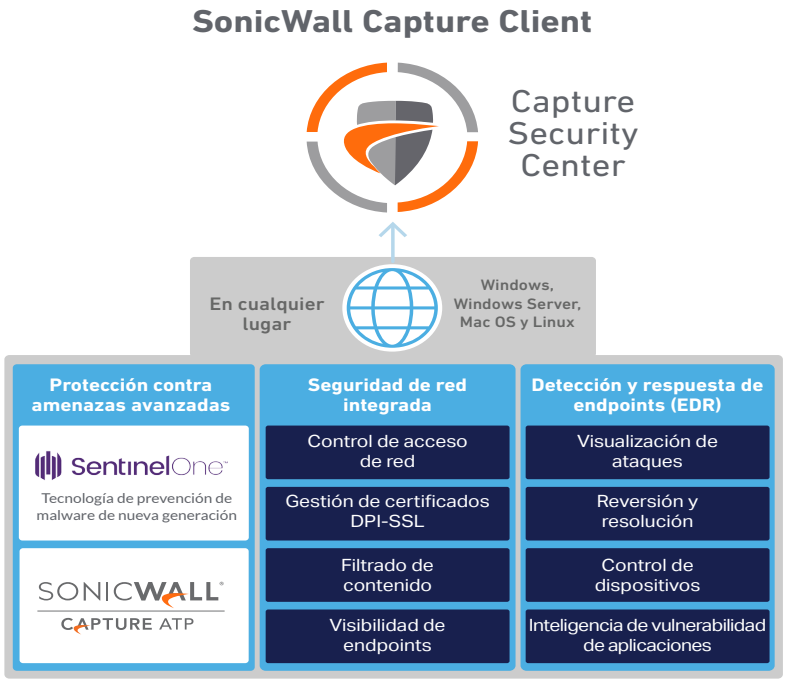
PRESTACIONES DESTACADAS

- Detección de amenazas altamente eficaz y accionable sin datos superfluos
- Gestión centralizada y basada en la nube con verdaderas prestaciones multiempresa para reforzar la seguridad de la red y de los endpoints
- Empodere y mejore los equipos de seguridad y TI con una solución intuitiva fácil de usar que detiene a los perpetradores de ataques modernos

Seguridad de endpoints adaptada a su organización

Lea el resumen: sonicwall.com

DATASHEET



Capture Client aplica protección avanzada contra las amenazas en base al comportamiento utilizando las prestaciones de NGAV SentinelOne.

Integración de Capture ATP para una mayor efectividad de la seguridad, tiempos de respuesta más rápidos y un menor coste total de propiedad

Prestaciones y ventajas

Monitorización continua del comportamiento

- Vea perfiles completos de la actividad de los archivos, las aplicaciones, los procesos y la red
- Proteja la red contra el malware basado en archivos y sin archivos
- Proporcione una visión de los ataques de 360 grados con inteligencia accionable

Caza de amenazas con visibilidad profunda

- Utilice visibilidad profunda para detectar amenazas en base a indicadores de comportamiento e indicadores de compromiso (IOC)
- Automatice la caza de amenazas y la respuesta con normas y alertas personalizadas

Integración con Capture Advanced Threat Protection (ATP)

- Cargue automáticamente los archivos sospechosos encontrados en dispositivos Windows para su análisis avanzado de sandboxing
- Encuentre amenazas latentes antes de que se ejecuten, como el malware con mecanismo de retardo integrado
- Consulte la base de datos de veredictos de archivos de Capture ATP sin necesidad de cargar archivos a la nube

Prestaciones únicas de reversión

- Soporte políticas que eliminen completamente las amenazas
- Restaure endpoints de forma autónoma restableciendo el buen estado conocido de antes de que se iniciara la actividad maliciosa

Múltiples técnicas multicapa basadas en heurística

- Utilice inteligencia en la nube, análisis estáticos avanzados y protección dinámica del comportamiento
- Proteja la red contra el malware conocido y desconocido y remédielo antes, durante y después de un ataque

Inteligencia de vulnerabilidades de las aplicaciones

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

Control de red en los endpoints

- Añada controles tipo firewall en el endpoint
- Utilice una base de normas de cuarentena para los dispositivos infectados

Remote Shell[1]

- Elimine la necesidad de tener contacto físico con los dispositivos para resolver problemas, cambiar configuraciones locales y realizar investigaciones forenses

No es necesario realizar escaneos regulares ni actualizaciones periódicas

- Permita el máximo nivel de protección en todo momento sin que la productividad de los usuarios se vea afectada
- Proporciona un escaneo completo en el momento de la instalación y posteriormente ofrece monitorización continua en busca de actividades sospechosas

Integración opcional con los firewalls de SonicWall

- Permita el refuerzo de la inspección profunda de paquetes de tráfico cifrado (DPI-SSL) en los endpoints
- Implemente fácilmente certificados de confianza en cada endpoint
- Dirija a los usuarios no protegidos a una página de descarga de Capture Client antes de que accedan a Internet siempre que se encuentren detrás de un firewall

Filtrado de contenido

- Bloquee sitios, direcciones IP y dominios maliciosos
- Aumente la productividad de los usuarios limitando el ancho de banda o restringiendo el acceso a contenido Web cuestionable o improductivo

Control de dispositivos

- Bloquee dispositivos potencialmente infectados para evitar que se conecten a los endpoints
- Utilice políticas granulares para la elaboración de listas de dispositivos autorizados

Prestaciones de Capture Client		
Prestación	Advanced	Premier
Gestión, informes y análisis en la nube	✓	✓
Integraciones de seguridad de red		
Visibilidad y refuerzo de endpoints	✓	✓
Implementación de certificados DPI-SSL	✓	✓
Filtrado de contenido	✓	✓
Protección avanzada de endpoints		
Antimalware de nueva generación	✓	✓
Sandboxing Capture Advanced Threat Protection	✓	✓
ActiveEDR (Detección y respuesta para endpoints)		
Visualización de ataques	✓	✓
Reversión y resolución	✓	✓
Control de dispositivos	✓	✓
Vulnerabilidades e inteligencia de aplicaciones	✓	✓
Dispositivos no autorizados		✓
Control de red en los endpoints		✓
Caza e inteligencia de amenazas ActiveEDR		
Caza de amenazas con visibilidad profunda		✓
Remote Shell[1]		✓
Catálogo de exclusiones		✓

[1] Remote shell se pondrá a disposición bajo demanda en una nueva cuenta (con 2FA habilitado) directamente en la consola S1.

Capture Client - Requisitos del sistema | SonicWall

Mejores prácticas para las operaciones de seguridad global de endpoints para MSSPs y empresas distribuidas

Lea el resumen de la solución: www.sonicwall.com

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com