SonicWall Capture Advanced Threat Protection Service

Descubra y detenga las amenazas de día cero y otros ataques desconocidos

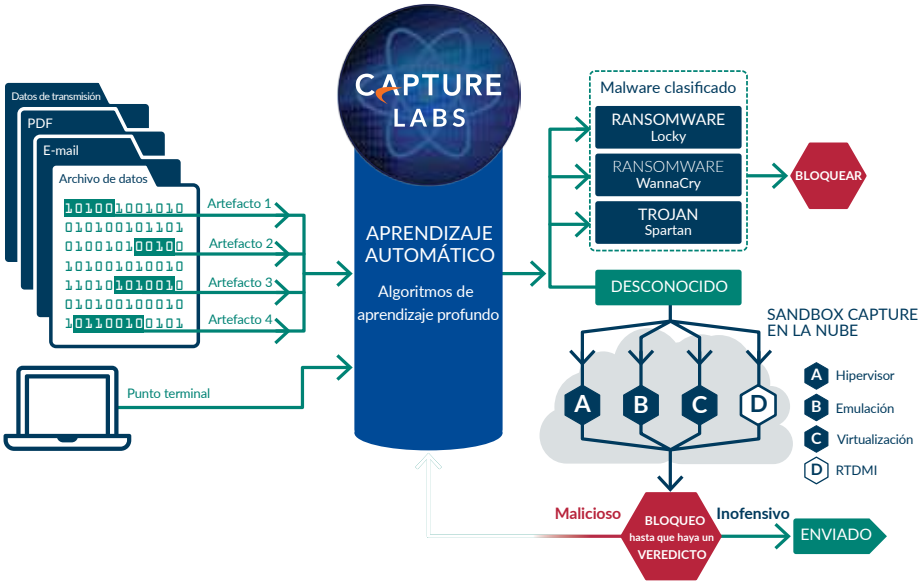
Para disfrutar de una protección efectiva contra las amenazas de día cero, las organizaciones necesitan soluciones que incluyan tecnologías de análisis de malware y que sean capaces de detectar las amenazas avanzadas y de malware evasivas, tanto a día de hoy como en el futuro.

Para proteger a los clientes contra los crecientes peligros de las amenazas de día cero, SonicWall Capture Advanced Threat Protection Service —un servicio basado en la nube disponible con los firewalls de SonicWall— detecta las amenazas y puede bloquearlas en la pasarela hasta que haya un veredicto. Se trata del único producto de detección de amenazas avanzadas que combina el sandboxing multicapa, incluida la Inspección de memoria profunda en tiempo real (RTDMI) de SonicWall, emulación del sistema completo y técnicas de virtualización, a fin de analizar comportamientos de código sospechosos. Gracias a esta eficaz combinación, SonicWall Capture Advance Threat Protection Service detecta más amenazas que las soluciones de sandbox de un solo motor, que son específicas de un entorno de computación y susceptibles a la evasión.

Esta solución escanea el tráfico y extrae el código sospechoso para analizarlo. Además, a diferencia de otras soluciones de pasarela, analiza una amplia variedad de tamaños y tipos de archivos. La infraestructura global de inteligencia de amenazas rápidamente implementa las definiciones de las amenazas recién identificadas en todos los dispositivos de seguridad de red de SonicWall, a fin de detener la infiltración. Los clientes se benefician de una seguridad altamente efectiva, tiempos de respuesta rápidos y un coste total de propiedad reducido.

Ventajas:

- Seguridad altamente efectiva contra amenazas desconocidas
- La implementación de definiciones casi en tiempo real protege contra posibles ataques derivados
- Coste total de propiedad reducido
- Bloqueo de archivos en la pasarela hasta que se emita un veredicto
- Múltiples motores procesan archivos en paralelo para acelerar los veredictos
- El motor RTDMI de SonicWall bloquea el malware desconocido del mercado de masas utilizando técnicas de inspección en tiempo real basada en memoria



Una solución multimotor basada en la nube para detener los ataques desconocidos y de día cero en la pasarela

Con el fin de ofrecer la mejor protección contra amenazas de día cero, la solución está diseñada para añadir nuevas tecnologías de análisis de malware de forma dinámica a medida que evoluciona el panorama de las amenazas.

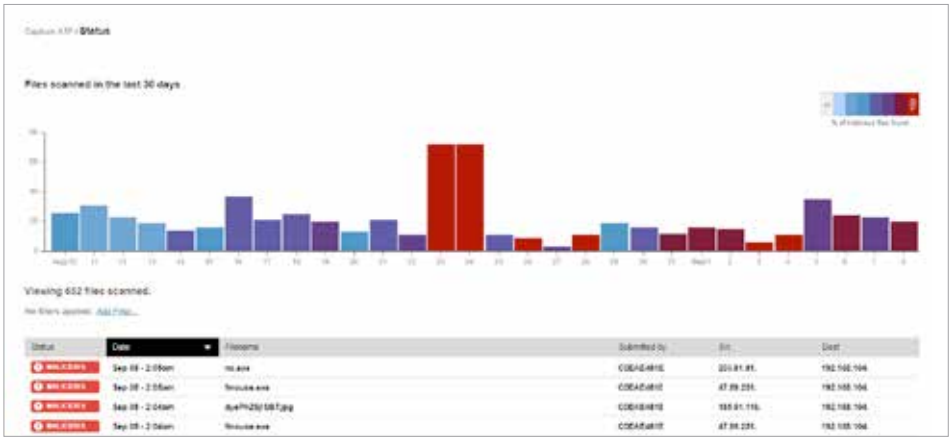
Prestaciones

Análisis multimotor de amenazas avanzadas — SonicWall Capture ATP Service amplía la protección antiamenazas de los firewalls para detectar y prevenir los ataques de día cero. El firewall inspecciona el tráfico y detecta y bloquea las intrusiones y el malware conocido. Los archivos sospechosos se envían al servicio de la nube de SonicWall Capture ATP para su análisis. La plataforma de sandbox multimotor, que incluye RTDMI, sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso, analiza su comportamiento y proporciona una visibilidad completa de la actividad maliciosa al tiempo que ofrece resistencia a las técnicas de evasión y maximiza la detección de amenazas de día cero.

Inspección profunda de la memoria en tiempo real (RTDMI) — El servicio multimotor Capture ATP de SonicWall se ve mejorado por nuestra tecnología pendiente de patente de Inspección de memoria profunda en tiempo real. El motor RTDMI detecta y bloquea de forma proactiva el malware desconocido del mercado de masas, las amenazas de día cero y el malware desconocido inspeccionando directamente en la memoria. Gracias a su arquitectura en tiempo real, la tecnología RTDMI de SonicWall es precisa, minimiza los falsos positivos e identifica y mitiga loas ataques sofisticados.

Análisis de gran variedad de tipos de archivos — Este servicio soporta el análisis de una amplia variedad de tamaños y tipos de archivos, incluidos programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows y Android. Los administradores pueden personalizar la protección seleccionando o excluyendo archivos para que sean enviados a la nube, donde se analizan por tipo de archivo, tamaño de archivo, remitente, destinatario o protocolo. Además, los administradores pueden enviar archivos manualmente al servicio en la nube para su análisis.

Bloqueo hasta que haya un veredicto — A fin de evitar el acceso a la red de archivos potencialmente peligrosos, los archivos enviados al servicio en la nube para su análisis pueden retenerse en la pasarela hasta que se emita un veredicto.



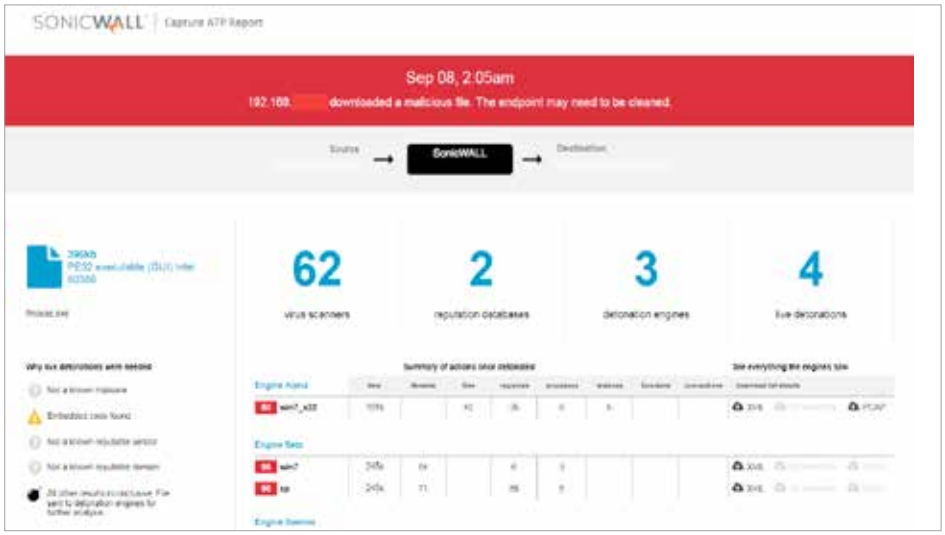
La página de informes de SonicWall Capture ATP muestra resultados diarios de un vistazo. Las barras de colores que aparecen en el informe indican los días en que se ha descubierto malware. Los administradores pueden hacer clic en los resultados diarios individuales y aplicar filtros para ver rápidamente los archivos maliciosos con los correspondientes resultados.

Rápida implementación de definiciones — Cuando se detecta un archivo malicioso, inmediatamente se pone a disposición una definición para los firewalls con suscripción a SonicWall Capture ATP con el fin de evitar posibles ataques derivados. Además, el malware se envía al equipo de investigación de amenazas de SonicWall Capture Labs para ser analizado con mayor detalle e incluido, junto con información sobre la amenaza, en las bases de datos de definiciones de Gateway Anti-Virus e IPS. Asimismo, en el transcurso de 48 horas, se envía a bases de datos de reputación de URL, IP y dominios.

Informes y alertas — SonicWall Capture ATP Service proporciona informes y un cuadro de mando de análisis de amenazas de un solo vistazo con información detallada sobre los resultados del análisis de los archivos enviados al servicio (origen, destino y un resumen con detalles de la acción del malware tras su detonación). Las alertas de registro del firewall proporcionan notificaciones sobre los archivos sospechosos enviados a SonicWall Capture ATP Service, y sobre el veredicto del análisis de los mismos.

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.



También hay disponible un informe de análisis detallado de los archivos analizados para facilitar la resolución.

PLATAFORMAS SOPORTADAS

Los siguientes firewalls de SonicWall —con SonicOS 6.2.6 y superior— soportan SonicWall Capture ATP Service:

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

Serie TZ600
Serie TZ500
Serie TZ400
Serie TZ300

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

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

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG4093