Symantec
A Division of Broadcom

Descripción del producto

Symantec Endpoint Security

Ahora, implementar una estrategia integral de seguridad de los endpoints es más importante que nunca.

Introducción

Los endpoints son el principal objetivo de los atacantes cibernéticos. A medida que se intensifican las consecuencias y los daños ocasionados por los ataques exitosos, muchas empresas intentan fortalecer su defensa en general mediante la incorporación de múltiples productos para la protección de endpoints. Lamentablemente, este enfoque conduce a un debilitamiento de la postura en materia de seguridad de la organización

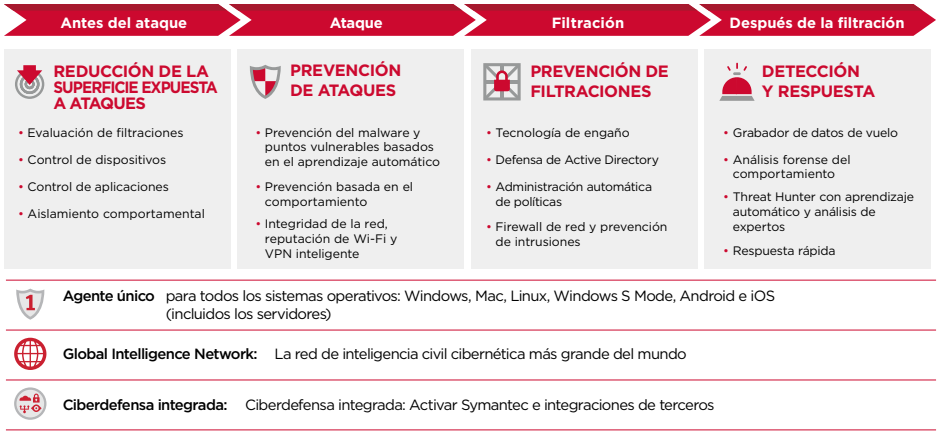
Según Ponemon Institute, las organizaciones instalan, en promedio, siete agentes de endpoint distintos para brindar soporte a la gestión y la seguridad de TI[1]. Cada agente opera de manera independiente con su propia consola y su conjunto de reglas y políticas exclusivos, que deben configurarse, implementarse, administrarse y mantenerse. Además de generar más gastos generales y costos de TI, la incorporación de múltiples productos conduce a brechas y errores en la defensa. De esta manera, se incrementan las posibilidades de pasar por alto una amenaza.

La prevención cobra una importancia cada vez mayor a medida que las amenazas cibernéticas globales son más agresivas que nunca y ejercen un impacto asombroso sobre el negocio. Una empresa por completo podría verse comprometida en el mismo tiempo que le lleva leer este resumen del producto. El ataque NotPetya desmanteló por completo una de las más grandes compañías navieras del mundo en tan solo 7 minutos[2], junto con miles de otras organizaciones. Resulta fundamental prevenir los ataques tan pronto sea posible, ya que la ventana de detección y reacción ante un ataque moderno es muy acotada. Asimismo, es muy importante invertir en respuesta ante incidentes para adoptar una postura de seguridad fortalecida que permita evitar ataques futuros. Symantec le permite dejar atrás estos problemas. ¿Por qué elegir entre el mejor nivel de seguridad y la mayor simplicidad cuando puede tener ambos?

Funciones destacadas de Symantec Endpoint Security Complete

- Protección para todos los endpoints: equipos portátiles, equipos de escritorio, tablets, dispositivos móviles y servidores
- Agente único para la reducción de la superficie expuesta a ataques, prevención de ataques, prevención de filtraciones y Detección y respuesta de endpoints (EDR)
- Consola única con visibilidad de amenazas en tiempo real
- Implementación flexible: en las instalaciones, administrada en la nube y modelos híbridos
- Seguridad de Active Directory
- Capacidades de aislamiento comportamental y control de aplicaciones
- Gestión de la seguridad guiada por la inteligencia artificial (IA)
- Análisis de ataques dirigidos y Threat Hunter
- Global Intelligence Network (GIN), uno de los más importantes a nivel mundial, ofrece información sobre amenazas, análisis de amenazas, clasificación de contenidos y datos integrales para el bloqueo de amenazas en tiempo real
- Integración con aplicaciones de terceros, como Microsoft Graph, Open C2 y otras soluciones de Symantec a través de Symantec ICDx

Figura 1: Symantec Endpoint Security Complete



1: The 2017 State of Endpoint Security Risk (El estado del riesgo de la seguridad de los endpoints), Ponemon Institute LLC, noviembre de 2017.

2: *You're Just 7 Minutes Away from an Infinite Toxic Loop in Your Network (Está a tan solo 7 minutos de sufrir un bucle tóxico infinito en su red)*, blog de Symantec, abril de 2019.

Versión Enterprise Funciones destacadas

- Protege equipos portátiles, equipos de escritorio, teléfonos móviles y tablets
- Agente único para la seguridad de endpoints
- Consola única con visibilidad de amenazas en tiempo real
- Implementación flexible: en las instalaciones, administrada en la nube y modelos híbridos
- Gestión de la seguridad guiada por la inteligencia artificial (IA)
- Global Intelligence Network, uno de los más importantes a nivel mundial, ofrece información sobre amenazas en tiempo real
- Integración con aplicaciones de terceros, como Microsoft Graph, Open C2 y otras soluciones de Symantec a través de Symantec Integrated Cyber Defense Exchange (ICDx)

Descripción general de la solución

Symantec Endpoint Security Complete ofrece la plataforma de seguridad para endpoints más completa e integrada del mundo. Como solución en las instalaciones, híbrida o basada en la nube, la plataforma de agente único de Symantec protege todos sus dispositivos de endpoint tradicionales y móviles, a la vez que ofrece defensas interconectadas a nivel del dispositivo, la aplicación y la red, además de utilizar inteligencia artificial (IA) para optimizar la toma de decisiones sobre seguridad. Un sistema unificado de administración basado en la nube simplifica la protección, la detección y la respuesta ante todas las amenazas avanzadas dirigidas a sus endpoints.

Seguridad de endpoints inigualable para su empresa
Symantec Endpoint Security le brinda a su organización el mejor nivel de seguridad en los endpoints, tanto para dispositivos móviles como tradicionales, en las tres etapas de ataque (previa al ataque, ataque y posterior al ataque) y hace hincapié en la prevención en la cadena de ataque para agilizar la contención. Sus innovadoras tecnologías de prevención y reducción de la superficie expuesta a ataques proporcionan la defensa más sólida para detectar las amenazas más complejas que utilizan métodos de ataque como el software malicioso furtivo, el robo de credenciales, los ataques sin archivos y los ataques LotL (Living off the Land). Symantec también previene las filtraciones masivas de datos antes de que se produzcan. Los análisis de ataques sofisticados, el análisis forense sobre el comportamiento, los manuales sobre investigación automatizada, la prevención de movimientos laterales y del robo de credenciales proporcionan una detección precisa de los ataques y la búsqueda proactiva de amenazas para contener las acciones de los atacantes y resolver las amenazas persistentes en tiempo real.

Reducción de la superficie expuesta a ataques

Symantec ofrece defensa proactiva de los endpoints con funciones de reducción de la superficie expuesta antes del ataque basadas en controles de políticas y tecnologías avanzadas que realizan búsquedas constantes para detectar la presencia de puntos vulnerables y configuraciones erróneas en aplicaciones, Active Directory y dispositivos. Si se aplican medidas de defensa para la reducción de la superficie expuesta a ataques en los endpoints, muchas de las tácticas y técnicas de los atacantes resultarán inútiles.

- La **evaluación de filtraciones** sondea Active Directory constantemente para detectar configuraciones erróneas de los dominios, vulnerabilidades y la persistencia mediante el uso de simulaciones de ataques con el fin de identificar riesgos para proceder a la mitigación inmediata con recomendaciones prescriptivas sobre soluciones.
- El **control de dispositivos** establece el bloqueo o la autorización de políticas en los diferentes tipos de dispositivos que se conectan a equipos cliente como USB, infrarrojos y FireWire para reducir el riesgo de amenazas y exfiltraciones.
- El **control de aplicaciones** evalúa el riesgo de las aplicaciones y sus vulnerabilidades, y permite que solo se ejecuten aplicaciones conocidas.
- El **aislamiento comportamental** limita los comportamientos inusuales y riesgosos de las aplicaciones confiables con un impacto mínimo sobre las operaciones.
- La **reparación de vulnerabilidades**[3] mejora el nivel de seguridad, ya que proporciona visibilidad e inteligencia respecto de los puntos vulnerables y los riesgos asociados. Las vulnerabilidades detectadas se clasifican según su gravedad tomando como referencia el CVSS (Sistema de calificación de vulnerabilidades comunes), junto con la identificación de la cantidad de dispositivos afectados, con el objetivo de garantizar que se solucionen primero las amenazas más críticas.

3: Compatible con Windows 10, Windows 10 en S Mode y dispositivos Android, únicamente.

Prevención de ataques

La prevención de ataques de varias capas de Symantec protege de manera inmediata y eficaz contra los métodos y vectores de ataque basados en archivos y sin archivos. El aprendizaje automático y la inteligencia artificial emplean avanzados esquemas de detección basados en la nube y en dispositivos. El objetivo es identificar las amenazas que evolucionan para atacar diferentes tipos de dispositivos, sistemas operativos y aplicaciones. Los ataques se bloquean en tiempo real para mantener la integridad de los endpoints y evitar repercusiones negativas.

- La **prevención del malware** combina la detección y el bloqueo previos a la ejecución de amenazas nuevas y en evolución (aprendizaje automático avanzado, entorno de prueba aislado para detectar malware oculto en paquetes personalizados y monitoreo y bloqueo del comportamiento de archivos maliciosos) y métodos basados en firmas (análisis de la reputación de archivos y sitios web, y exploración de malware).
- La **prevención de puntos vulnerables** bloquea los ataques de día cero basados en memoria sobre los puntos vulnerables de software popular.
- La **protección intensiva** permite ajustar en detalle el nivel de detección y bloqueo por separado para optimizar la protección y mejorar la visibilidad de los archivos sospechosos.
- La **seguridad de las conexiones de red** identifica las redes Wi-Fi maliciosas; utiliza tecnología de reputación de punto de acceso y proporciona una VPN basada en políticas para proteger las conexiones de red y asegurar el cumplimiento.

Prevención de filtraciones

El enfoque de prevención de Symantec se orienta a contener a los atacantes tan pronto sea posible (en el endpoint) antes de que tengan la posibilidad de adentrarse en la red. Se ponen en funcionamiento diversas tecnologías de prevención de intrusiones y decepción basadas en la IA que frustran el ingreso en la red antes e inmediatamente después de que el endpoint se haya visto comprometido, es decir, antes de que se produzca una filtración de amplio alcance.

- El **firewall y la prevención de intrusiones** bloquean ataques de software malicioso conocidos basados en red y en navegador mediante reglas y políticas. Mediante la creación automática de listas negras de direcciones IP de dominios, también impiden la configuración de comandos y controles.
- La **tecnología de engaño** utiliza señuelos y cebos (archivos, credenciales, carpetas compartidas en red, entradas de memoria caché, solicitudes web y endpoints falsos) para exponer, detectar las tácticas y las intenciones de los atacantes, y demorar sus acciones mediante la visibilidad anticipada.
- La **seguridad de Active Directory** protege la superficie principal expuesta a ataques contra la tecnología de movimiento lateral y el robo de credenciales de administrador de dominio controlando la percepción que el atacante tiene de los recursos de Active Directory (desde el endpoint) mediante ofuscación sin límites (creación de credenciales y recursos falsos). Mediante la ofuscación, el atacante se delata mientras interactúa con *activos falsos* o intenta utilizar credenciales de administrador de dominio en la percepción de Active Directory.
- Basadas en aprendizaje automático y asistidas por inteligencia artificial avanzada, las **políticas administradas automáticamente** combinan de forma exclusiva indicadores de peligro y anomalías históricas. El objetivo es adaptar constantemente las reglas y los umbrales de las políticas de endpoint, y mantenerlos al día y en consonancia con el nivel de riesgo actual de su organización.

Respuesta y reparación después de una filtración

Symantec combina tecnologías de detección y respuesta para endpoints con sus inigualables capacidades de análisis del centro de operaciones de seguridad para permitirle solucionar con rapidez los incidentes en los endpoints y minimizar las repercusiones de los ataques. La integración de las funciones de detección y respuesta para endpoints (EDR) en una arquitectura de un único agente (que cubre endpoints tanto tradicionales como modernos) no solo permite detectar con exactitud los ataques avanzados y proporciona análisis en tiempo real, sino que además permite buscar amenazas de manera proactiva, efectuar exámenes forenses y ejecutar medidas de reparación.

- El **análisis forense** ofrece la capacidad para registrar y analizar el comportamiento de los endpoints con el objetivo de identificar técnicas avanzadas de ataque que podrían estar utilizando aplicaciones legítimas para fines maliciosos. Estos datos se enriquecen con el marco de trabajo MITRE ATT&CK que orienta a los encargados de brindar una respuesta ante los incidentes durante las investigaciones.
- En Symantec EDR, se proporcionan herramientas de **detección avanzada de amenazas**, que incluyen manuales incorporados en los que se plasman las prácticas recomendadas de responsables avezados en detección de amenazas y detección de comportamientos anómalos. Quienes se ocupan de brindar respuesta ante un incidente pueden buscar en toda la organización para detectar IOC para incluir directamente en la consulta del endpoint.
- **Respuesta integrada** actúa directamente en el endpoint para reparar mediante la recuperación y eliminación de archivos, el aislamiento de endpoints y la creación de listas negras. Symantec EDR permite el envío automático de archivos identificados como sospechosos al aislamiento de procesos para realizar análisis completos en busca de software malicioso, incluido malware de exposición que detecta máquinas virtuales.

Respuesta y reparación después de una filtración (cont.)

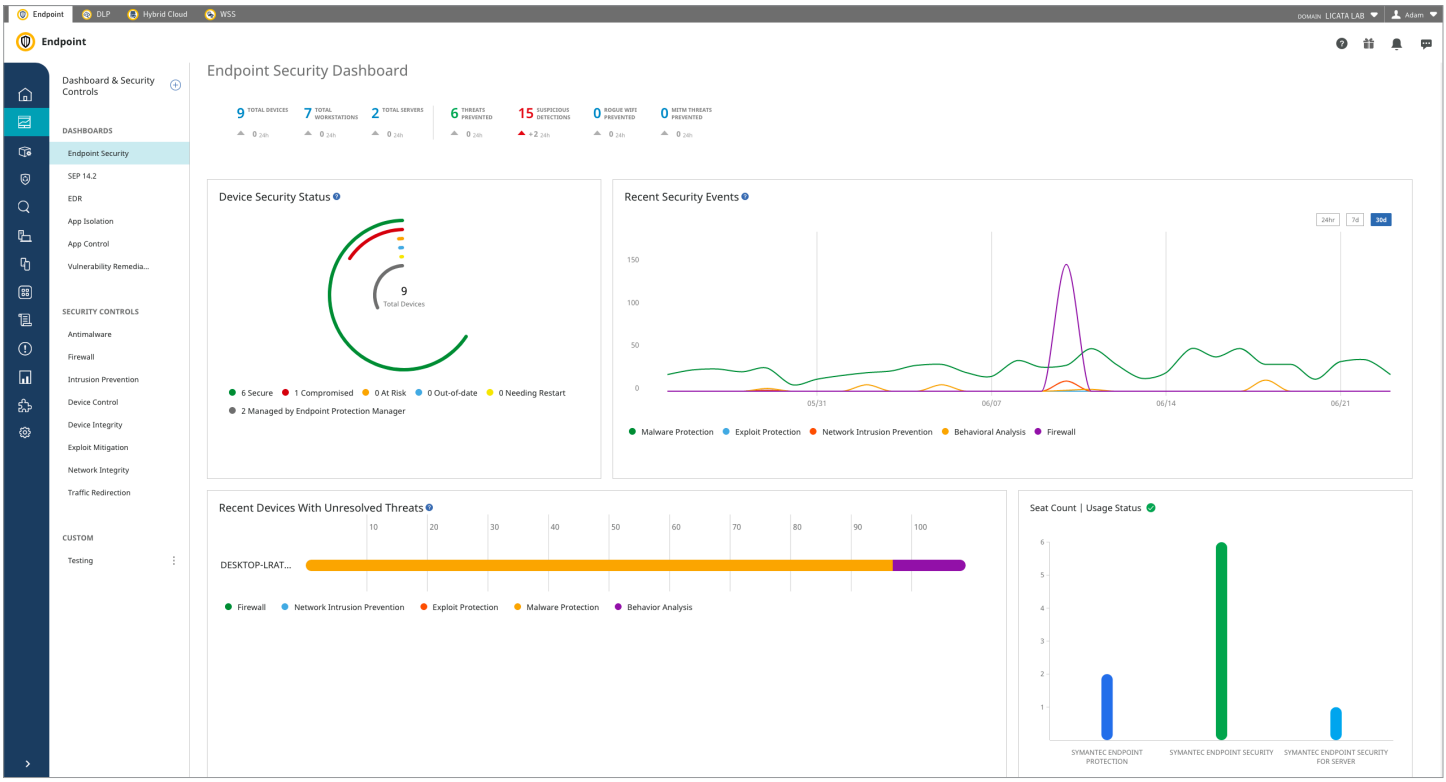
- **Threat Hunter** busca incidentes de alta fidelidad y combina el poder del aprendizaje automático avanzado y la participación de analistas expertos en SOC para detectar las herramientas, las tácticas y los procedimientos que utilizan los adversarios. Garantiza que los ataques críticos se identifiquen con rapidez en el contexto relevante. Asimismo, ofrece acceso intuitivo a los datos de seguridad global de Symantec para incrementar los esfuerzos de detección de amenazas de su equipo.
- **Respuesta rápida** permite reducir el tiempo necesario para reparar amenazas y ofrecer una respuesta a los atacantes en tiempo real. Las herramientas y los manuales incorporados permiten contener las amenazas al aislar a los atacantes y ofrecer acceso interactivo en los endpoints.

Proteja de manera sencilla su entorno dinámico de endpoints

Una pila de agente único permite reducir el impacto de la seguridad de los endpoints al mismo tiempo que integra (y coordina) las mejores tecnologías de prevención, detección y respuesta disponibles. Administre todo, desde un sistema único de gestión basado en la nube (Integrated Cyber Defense Manager). Así, podrá reducir el tiempo, los recursos y los esfuerzos necesarios para configurar, implementar, administrar y mantener su postura en cuanto a la seguridad. Puede acceder con tan solo uno o dos clics a todo lo que necesite, mejorar la productividad del administrador y agilizar los tiempos de respuesta para cerrar rápidamente los eventos de seguridad.

- La **administración de seguridad basada en la IA** permite actualizar las políticas con mayor precisión y tener una menor cantidad de configuraciones erróneas. Esto le permite mejorar su higiene de seguridad.
- Los **flujos de trabajo simplificados** garantizan que todo funcione a la perfección con el objetivo de incrementar el nivel de rendimiento, eficiencia y productividad.
- Las **recomendaciones que tienen en cuenta el contexto** contribuyen a alcanzar un rendimiento óptimo al eliminar las tareas de rutina y tomar mejores decisiones.
- La **gestión autónoma de la seguridad** toma información permanentemente de los comportamientos de administradores y usuarios con el objetivo de mejorar las evaluaciones de amenazas, ajustar las respuestas y fortalecer la postura general de su organización en cuanto a seguridad.

Figura 2: Interfaz de usuario del endpoint



Reducir la complejidad con las amplias integraciones de la cartera de Symantec y de terceros

Symantec Endpoint Security es una solución fundacional que facilita la integración, de manera tal que los equipos de seguridad de TI puedan detectar amenazas donde quiera que sea en su red y abordarlas con una respuesta organizada. Symantec Endpoint Security opera junto con otras soluciones de Symantec y productos de terceros por medio de aplicaciones específicas y API publicadas que permiten fortalecer la postura de seguridad de su organización. Ningún otro proveedor ofrece una solución integrada que permita organizar una respuesta en el endpoint (listas negras y reparaciones) desencadenada por la detección de una amenaza en las puertas de enlace de seguridad de la web y del correo electrónico. Entre las integraciones específicas, pueden mencionarse:

- **Symantec Web Security Service:** Redirige el tráfico web de los usuarios de roaming de Symantec Endpoint Security a Symantec Web Security Service y Symantec CASB mediante el uso de un archivo PAC.
- **Puerta de enlace web de Symantec:** Las API de REST programables posibilitan la integración con una infraestructura de seguridad de la red en las instalaciones.
- **Symantec Validation and ID Protection:** Autenticación de múltiples factores, que incluye tarjetas inteligentes PIV/CAC para consolas de administración en las instalaciones y basadas en la nube de Symantec Endpoint Security.
- **Symantec Content Analysis:** Utiliza un entorno de prueba aislado y dinámico en las instalaciones y motores adicionales de amenazas para realizar un análisis más detallado de los archivos sospechosos que se envían desde Symantec Endpoint Security.
- **Symantec Data Loss Prevention:** Evita la exfiltración de datos de información confidencial al proporcionarle a DLP inteligencia sobre amenazas en tiempo real de aplicaciones sospechosas.

Figura 3: Symantec Endpoint Security

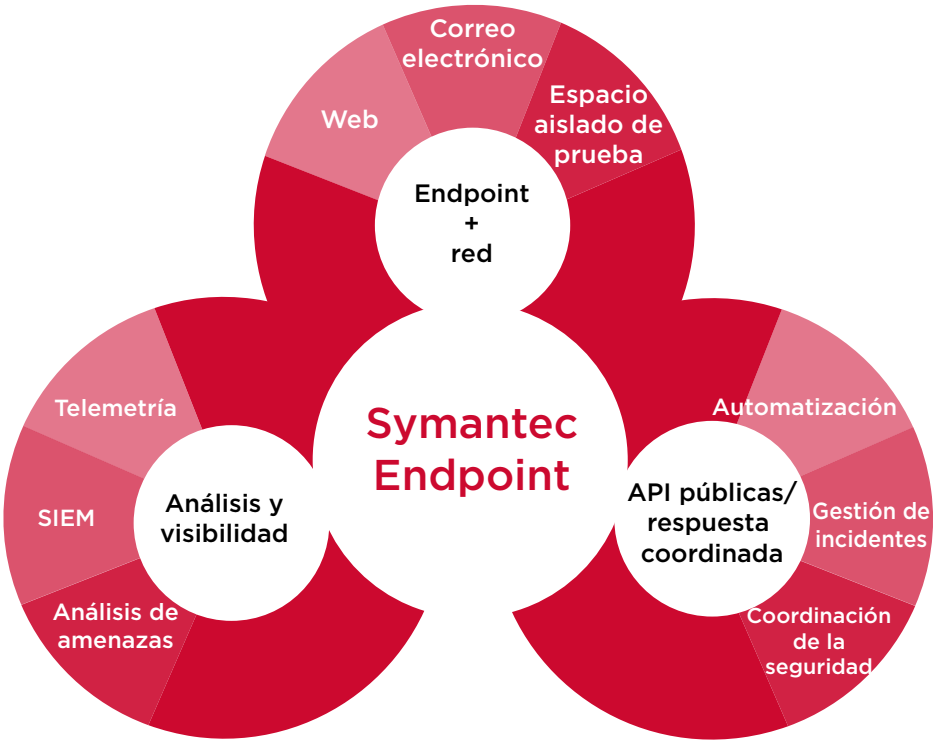


Figura 4: Opciones de licencias

Funciones

	SEP	SES ENTERPRISE	SES COMPLETE
	Estándar de la industria en protección de endpoints. Cinco años consecutivos como líderes en protección y, ahora, también en rendimiento, según AV Test.	Extiende SEP a todos los sistemas operativos y dispositivos, incluidos los dispositivos móviles. Ofrece gestión de la nube.	Aporta protección avanzada, EDR, detección de amenazas y otras tecnologías para una protección completa.
OPCIONES DE ADMINISTRACIÓN	En las instalaciones	En las instalaciones, Nube, Híbrida	
AGENTES REQUERIDOS	AGENTE SYMANTEC ÚNICO		
COBERTURA DE DISPOSITIVOS De propiedad corporativa, BYOD, UYOD	Equipo portátil, Equipo de escritorio, Servidor	Móvil, Tablet, Equipo portátil, Equipo de escritorio, Servidor	
COBERTURA DEL SO	Windows, macOS, Linux	Windows (incluye S Mode y Arm), macOS, iOS, Linux, Android	

Tecnologías de protección

	SEP	SES ENTERPRISE	SES COMPLETE
PREVENCIÓN DE ATAQUES			
LA MEJOR PREVENCIÓN DE ATAQUES DE LA INDUSTRIA	✓	✓	✓
MOBILE THREAT DEFENSE		✓	✓
CONEXIÓN SEGURA A LA RED		✓	✓
REDUCCIÓN DE LA SUPERFICIE EXPUESTA A ATAQUES			
EVALUACIÓN DE FILTRACIONES			✓
AISLAMIENTO COMPORTAMENTAL			✓
CONTROL DE APLICACIONES			✓
CONTROL DE DISPOSITIVOS	✓	✓	✓
PREVENCIÓN DE FILTRACIONES ...			
PREVENCIÓN DE INTRUSIONES	✓	✓	✓
CORTAFUEGOS	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
...PREVENCIÓN DE FILTRACIONES			
TECNOLOGÍA DE ENGAÑO	✓	✓	✓
SEGURIDAD DE ACTIVE DIRECTORY			✓
RESPUESTA Y REPARACIÓN			
DETECCIÓN Y RESPUESTA DE ENDPOINTS			✓
ANÁLISIS DE NUBE DE ATAQUES DIRIGIDOS			✓
ANÁLISIS FORENSE DEL COMPORTAMIENTO			✓
THREAT HUNTER			✓
RESPUESTA RÁPIDA			✓
OPERACIONES DE TI			
DESCUBRIR E IMPLEMENTAR	✓	✓	✓
COMPROBACIONES DE INTEGRIDAD DEL HOST	✓	✓	✓

Symantec™
A Division of Broadcom

Para obtener información del producto, visite nuestro sitio web en go.broadcom.com/ses

SED-EPS-PB101_ES_LA Jueves, 25 de junio de 2020