

Symantec Endpoint Security: protegiendo toda la cadena de ataque

El *endpoint* no siempre ha estado tan protegido como debiera y en algunos casos las soluciones implantadas no han sido las más adecuadas.

La pandemia nos ha traído una nueva realidad: la del teletrabajo masivo y la implantación del trabajo híbrido, con la implicación de mayores riesgos y nuevos desafíos desde el punto de vista de la seguridad, sobre todo para los sectores críticos, más expuestos a los ciberataques. La plataforma de seguridad de *endpoints* Symantec Endpoint Security resuelve estos desafíos, proporcionando una seguridad integral para todos los dispositivos de la compañía.

Inma Elizalde

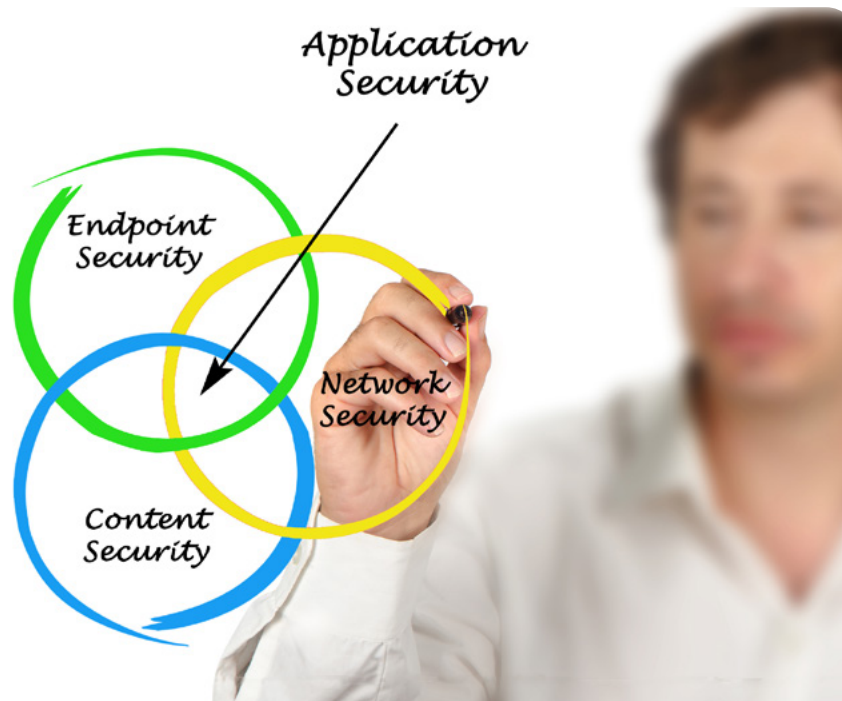
Los ciberdelincuentes siguen haciendo de los ataques a empresas y particulares un negocio, con el *ransomware* por bandera. Según un estudio publicado por Deloitte, el 94 % de las empresas sufrió, al menos, un incidente grave de ciberseguridad en 2021. Y un 69 % entre uno y dos ataques graves.

Junto al *ransomware*, el *malware* y el *phishing* se convierten en las principales amenazas, aumentando su nivel de sofisticación. A esto se suma el agravante de que muchas de las amenazas pueden combinarse en un mismo ataque, con el *phishing* como vector de entrada.

Por sectores el de seguros, TMT (telecomunicaciones, medios de comunicación y tecnología), fabricación, banca y Administración Pública sufren ataques por encima de la media.

Según un estudio llevado a cabo por IDC, ante la sofisticación de los mismos se ha producido un cambio notable en

las prácticas de seguridad del *endpoint* en los últimos años, originando una mayor capacidad de respuesta en las organizaciones. Algo necesario si tenemos en cuenta que el *endpoint* ha sufrido las consecuencias de contar con soluciones EPP (Plataforma de la Protección del Endpoint) inadecuadas, por lo que es aconsejable revisar las mismas para no comprometer los resultados esperados en su protección.



Una recomendación importante: antes de decidir sobre el mejor abordaje para una solución EDR, es conveniente evaluar las plataformas de protección utilizadas.

Symantec Endpoint Security

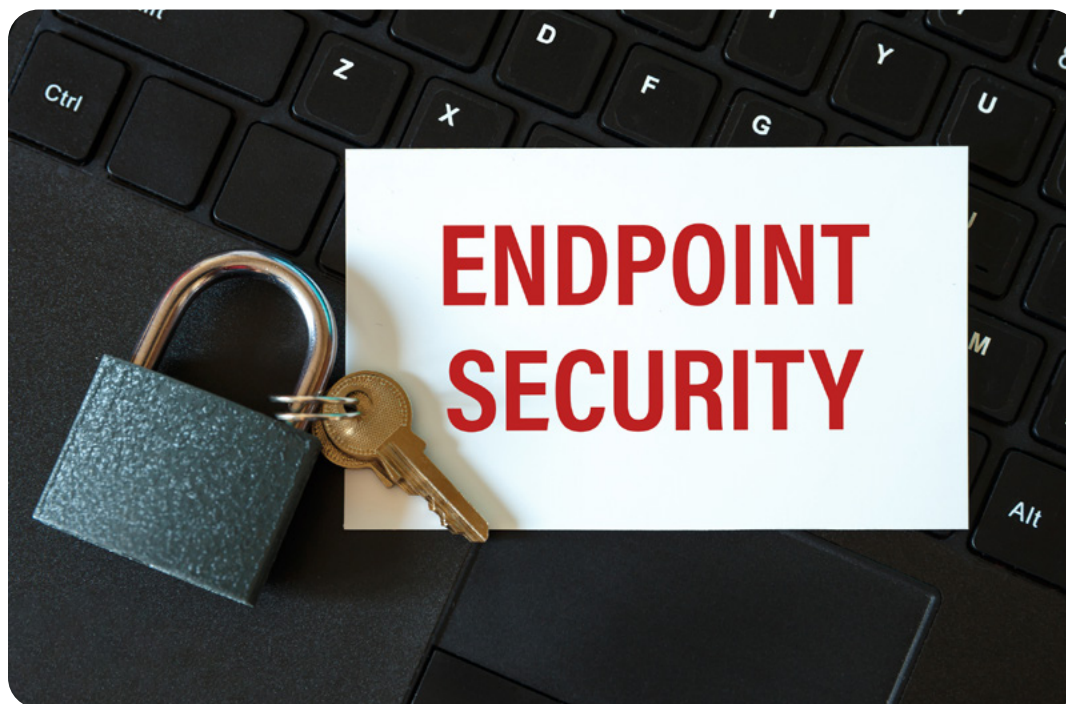
Broadcom, compañía especializada en tecnología de infraestructura, cuenta en su catálogo de ciberseguridad con una plataforma de seguridad integrada con el objetivo de proteger a las empresas de ciberamenazas. Dentro de la misma, la protección del *endpoint* juega un papel fundamental. Una protección englobada en tres soluciones:

- 1) SEP:** el conocido EPP de Symantec.
- 2) SES Enterprise (Symantec Endpoint Security):** su solución SaaS que se diferencia de la anterior tanto por su arquitectura como por contar con una licencia de SES: Mobile Threat Defense (que también puede consumirse en un dispositivo

móvil). Además de contar con la protección de ataques de red Secure Connections para usuarios que trabajan en áreas públicas y en redes no corporativas.

3) SES Complete, también en arquitectura *cloud*. Aquí se reúnen las capacidades de las dos anteriores más el EDR, la protección del directorio activo y el control y aislamiento de aplicaciones.

Symantec Endpoint Security ha aumentado y reforzado todos los componentes de su solución como la protección y defensa del directorio activo para movimientos laterales, ante la peligrosidad que supone para cualquier organización que un atacante solo tarde siete minutos en comprometer la seguridad del mismo. Sin olvidar otros elementos importantes como el control y aislamiento de aplicaciones o su EDR. Todo desde un único agente. Esto hace que disminuyan las dificultades



des que supone contar con varios agentes y el problema de rendimiento que esto conlleva. Todo ello sin olvidar que con Symantec Endpoint Security Complete se refuerzan las políticas de conformidad para todos los usuarios, independientemente de su ubicación o del dispositivo. Una opción a la hora de respaldar la productividad y afianzar la seguridad frente a las amenazas cambiantes.

"Las funcionalidades de Symantec Endpoint Security ofrecen una reducción de la superficie de ataque"

Fases

La protección contra los ataques no debe llevarse a cabo cuando ya es demasiado tarde. Es imprescindible contar con soluciones que nos protejan durante el mismo, pero la solución debe prevenir antes de que este se produzca. Esto también lo lleva a cabo Symantec Endpoint Security con su línea de protección

"La experiencia de usuario es algo que Symantec Endpoint Security cuida al máximo"



basada en cuatro fases: antes y durante el ataque, en la fase del incumplimiento y tras el post incumplimiento. Las cuatro emplean tecnologías enfocadas en la reducción de la superficie de ataque con el control de dispositivos o el aislamiento de la conducta, pasando por la detección y respuesta.

El producto cuenta con el uso de Global Intelligence Network para tener el conjunto más amplio de inteligencia. Y con Symantec Integrated Cyber Defense, que aloja la consola de manejo *cloud* (ICDm).

Protección del *endpoint* híbrido

Con la implantación del trabajo híbrido hay que focalizar las soluciones de ciberseguridad en el *endpoint* híbrido para cubrir todos los movimientos del mismo. ¿Qué retos se le presentan al CIO y al CISO en este sentido? Entre los principales desafíos a los que tienen que hacer frente se encuentran los usuarios, la tecnología que se emplea para trabajar en remoto, los servicios en la nube y los dispositivos IoT.

Para resolver estos desafíos la protección de la solución ya no está vinculada a contar con agentes centralizados en el perímetro, ya que con la arquitectura en modo SaaS de Symantec Endpoint Security es posible estar descentralizados y protegidos, incluso sin tener acceso puntual a la consola de manejo *cloud* (ICDm). Y con tecnologías como LiveUpdate y protecciones a nivel de seguridad de conexión el agente analiza, gracias a la red de inteligencia global,

si un AP público es susceptible de ser malicioso, levantando una *smart* VPN para protegernos.

Inmejorable experiencia de usuario

La experiencia de usuario es algo que Symantec Endpoint Security cuida al máximo al crear, para el departamento de IT, una solución intuitiva que permite una gestión ágil, con una interfaz unificada con varios productos de Symantec Cloud. Y para los usuarios, un agente ligero que no requiere de una atención especial.

Reconocimientos de grandes consultoras

Todo ello ha hecho que las soluciones de Symantec figuren entre las de los fabricantes destacados en el entorno del *endpoint* por parte de consultoras como Gartner, Forrester o Radicati, por poner algunos ejemplos. Según informes publicados por las mismas, los líderes de seguridad y gestión de riesgos responsables de la protección de *endpoints* valoran las capacidades de detección de amenazas avan-

zadas y las funcionalidades de investigación y remediación.

Las funcionalidades de Symantec Endpoint Security ofrecen una reducción de la superficie de ataque (incluido el aislamiento de aplicaciones, control de aplicaciones y seguridad de *active directory*), una pila de tecnología preventiva

completa y detección y respuesta avanzadas, junto con analistas expertos en ciber SOC.

La solución cubre los puntos finales tradicionales y los dispositivos móviles modernos, con opciones administradas en la nube, locales e híbridas. Todo ello a través de un agente único que agiliza la operativa.

A tener en cuenta

- Esta plataforma de seguridad de *endpoints* ofrece protección basada en la nube, con administración de seguridad guiada por IA.
- Permite descubrir y resolver las amenazas con una gran visibilidad de los *endpoints*, llevando a cabo un análisis en profundidad.
- Aborda las amenazas en toda la cadena de ataque.
- Protege a empleados corporativos y remotos.
- Reduce los tiempos de remediación.
- Recopila información global sobre amenazas de organizaciones de todos los tamaños.
- Identifica los primeros signos de ataques ocultos en una organización y notifica al SOC a través de la consola SES Complete.
- La solución es escalable.
- Ofrece un retorno de la inversión del 437 %, según la consultora Forrester.