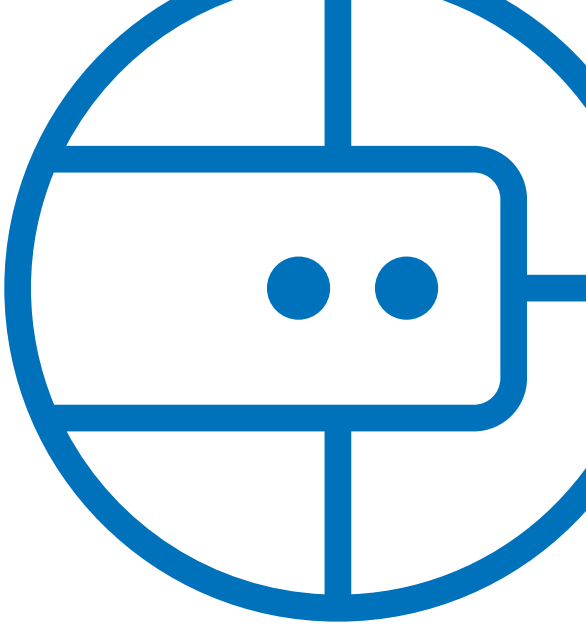
SOPHOS



Guía para la adquisición de Server Protection

Las ciberamenazas contra los servidores siguen evolucionando tanto en complejidad como en virulencia a un ritmo alarmante. Los devastadores ataques de ransomware como el WannaCry y el NoPetya han puesto de relieve la necesidad de contar con funciones antiransomware potentes. Las vulnerabilidades sistémicas explotadas por ataques como el Spectre y el Meltdown demostraron que el control antiexploits y de aplicaciones y los instrumentos de investigación como la EDR son clave en cualquier plan de seguridad para servidores.

Los servidores suelen ser los endpoints más valiosos de cualquier organización, por lo que es apremiante para los directores de TI seleccionar una protección altamente efectiva. No basta con ejecutar una solución de seguridad creada para dispositivos de escritorio en sus servidores; se necesitan soluciones diseñadas específicamente con la protección de cargas de trabajo de servidores como prioridad.

El objetivo de esta guía es ofrecerle asesoramiento práctico sobre funciones y características clave que debe considerar al seleccionar un producto de seguridad para sus servidores, además de las preguntas que debe hacer a los proveedores para asegurarse de que el funcionamiento de las prestaciones sea exactamente el esperado.

Entornos de servidor

En función de las necesidades de su empresa, puede que esté ejecutando servidores propios localmente,

alojando sus datos en la nube pública, como Amazon Web Services (AWS), Microsoft Azure o la nube de Google, o utilizando una combinación de estas opciones. Lo que necesita como mínimo es una solución de seguridad que le permita gestionar fácilmente estos distintos despliegues de manera integrada.

Lo ideal es una solución que ofrezca ventajas añadidas, como una implementación de políticas uniforme en todos los servidores que se pueda gestionar de forma centralizada. El despliegue automatizado (por ejemplo, a través de scripts) de la protección de servidores en la nube es fundamental para que pueda incrementarse (o disminuirse) su rendimiento cuando sea necesario para ajustarse a la demanda, sin que tenga que intervenir el administrador del servidor.

Y las opciones de licencias simplificadas son más importantes que nunca, ya que las organizaciones optan por entornos de despliegue mixtos. Busque un proveedor que ofrezca un único tipo de licencia, ya sea en la nube, localmente o una mezcla de ambos, y así se ahorrará un complejo proceso combinatorio.

Funciones y características claves del producto

La seguridad para servidores de hoy día ha evolucionado para anticiparse a las amenazas cada vez más avanzadas. Para mantener seguros sus servidores, ya sea localmente o en la nube, busque una serie de funciones que le protejan de amenazas desconocidas, ransomware, exploits y hackers:

- **Antiransomware**: algunas soluciones incluyen técnicas diseñadas específicamente para impedir el cifrado malicioso de datos por parte del ransomware. A menudo, las técnicas que son específicamente antiransomware también corrigen los archivos afectados revirtiéndolos a un estado normal, por ejemplo. Las soluciones antiransomware no solo deben detener el ransomware dirigido contra archivos, sino también el ransomware de discos utilizado en los destructivos ataques wiper que manipulan el registro de arranque maestro. Y en particular en el caso de los servidores, es necesario impedir que endpoints remotos o no autorizados cifren archivos en recursos compartidos de red u otros servidores conectados.
- **Bloqueo de servidor/listas blancas/denegación por defecto**: impida que aplicaciones no autorizadas se ejecuten en sus servidores creando listas blancas de aplicaciones permitidas. Los compradores deben buscar una solución que pueda identificar automáticamente las aplicaciones de confianza y que también permita la personalización por parte del usuario a fin de minimizar el tiempo y el esfuerzo requeridos para crear un conjunto de reglas seguro. Asimismo, el bloqueo y desbloqueo de un servidor no deberían implicar ningún tiempo de inactividad.
- **Antiexploits**: la tecnología antiexploits está diseñada para repeler a los atacantes bloqueando las herramientas y las técnicas de las que dependen en la cadena de ataque. Por ejemplo, exploits como el EternalBlue y el DoublePulsar se utilizaron para ejecutar el ransomware NotPetya y WannaCry. La tecnología antiexploits detiene el conjunto relativamente pequeño de técnicas utilizadas para propagar el malware y perpetrar ataques, lo que rechaza muchos ataques de día cero sin haberlos visto previamente y sin necesidad de firmas. La prevención de exploits exhaustiva también ofrece protección para servidores a los que no se puede aplicar parches de seguridad rápidamente, e incluso cuando no hay parches disponibles.

[1] Los 10 principales proyectos de seguridad de Gartner para 2018

- **Detección y respuesta para endpoints (EDR)**: la EDR ofrece a los administradores de TI la posibilidad de buscar amenazas esquivas de forma proactiva y profundizar en los incidentes de seguridad para comprender su alcance e impacto. Lo ideal es que la solución elegida incluya EDR que le ayude a centrarse en las áreas que le interesan, reduciendo la cantidad de datos que tiene que analizar y proporcionando información sobre archivos sospechosos para ayudarle a tomar una decisión informada.
- **Antihackers**: los servidores son uno de los principales objetivos de los hackers, ya que normalmente contienen los datos más confidenciales de una organización. Busque soluciones que cuenten con funciones específicas para detener ataques recurrentes de hackers que se producen en tiempo real. Algunos ejemplos de mitigaciones antihacker necesarias para servidores incluyen la prevención de recopilación de credenciales, prevención de movimientos laterales, mitigación de cuevas de código, protección contra el aumento de privilegios y protección contra la migración de procesos.
- **Machine Learning**: existen diversos tipos de métodos de Machine Learning, como las redes neuronales de Deep Learning, bosques aleatorios, análisis bayesianos y agrupación en clústeres. Independientemente de la metodología, los motores de detección de malware con Machine Learning deben diseñarse para detectar malware tanto conocido como desconocido sin depender de firmas. La ventajas del Machine Learning es que puede detectar malware nunca antes visto, lo que incrementa de forma óptima la tasa general de detección de malware. Las organizaciones deben evaluar la tasa de detección, el índice de falsos positivos y el impacto sobre el rendimiento de las soluciones basadas en Machine Learning.
- **Respuesta ante incidentes/Seguridad Sincronizada**: las herramientas para servidores deben proporcionar un mínimo de visibilidad sobre los hechos ocurridos a fin de evitar futuros incidentes. Lo ideal es que respondan de forma automática a los incidentes, sin necesidad de que intervengan los analistas, para evitar que las amenazas se propaguen o provoquen más daños. Es importante que las herramientas de seguridad del servidor se comuniquen con las demás herramientas de seguridad de la red como el firewall para detectar servidores en peligro y ofrecer visibilidad de todas las aplicaciones que se ejecutan en el servidor.
- **Monitorización de integridad de archivos**: debe proteger los datos y archivos críticos del sistema de cualquier cambio no intencionado y, de manera opcional, supervisar las ubicaciones clave de las aplicaciones. Sophos Central Server Protection supervisa y realiza un seguimiento continuo de los cambios imprevistos e inesperados para ayudar a identificar posibles infracciones de seguridad del estándar PCI DSS.
- **Control de aplicaciones**: ofrece control sobre qué aplicaciones tienen permiso para ejecutarse en el servidor a fin de reducir la superficie de ataque. Lo ideal es que el proveedor filtre las aplicaciones por categoría para simplificar y acelerar la configuración.
- **Gestión centralizada**: la consola debe hacer posible una gestión y una visibilidad sencillas de los entornos de servidor mixtos; por ejemplo, que permita el filtrado de todas las alertas, eventos e informes en una única vista de fácil acceso y fácil de entender.
- **Detección y protección de cargas de trabajo**: la protección en la nube depende de la protección de cada instancia o equipo virtual (VM) y de cada bucket de almacenamiento. La detección de cargas de trabajo y buckets de almacenamiento que se ejecutan en entornos en la nube pública como Amazon Web Services (AWS) y Microsoft Azure es fundamental, porque se sabe que los atacantes aprovechan las regiones sin utilizar de la nube y las readaptan, por ejemplo, para la criptominería. Los productos con integración de API nativa con plataformas en la nube pública muestran nuevas instancias de cargas de trabajo y almacenamiento, incluso en aquellas regiones que no se utilizan activamente.

Gestión e informes

La mayoría del tiempo no se inicia sesión en los servidores; solo suele hacerse cuando hay algún problema. Esto significa que, en materia de gestión, existen dos requisitos principales:

1. Un despliegue y una supervisión sencillos de todos los servidores
2. Una interfaz fácil de utilizar que permita responder rápidamente si se produce un problema

En muchos casos, desplegar soluciones puntuales de múltiples proveedores para distintos servidores en entornos diferentes puede provocar problemas de gestión debido a la existencia de múltiples consolas. Esto puede convertirse rápidamente en un verdadero lastre al tratar con entornos de servidores de mayor tamaño. Responder a un ataque grave requiere una acción rápida y decidida que no se vea obstaculizada por el tiempo que se desperdicia tratando de localizar información crítica necesaria para tomar una decisión. Busque soluciones que consoliden la información en un único panel intuitivo que simplifique al máximo la localización de los datos importantes.

Algunas soluciones también ofrecen la posibilidad de integrar su servidor en su seguridad de red (firewall) y compartir la información sobre amenazas. Por ejemplo, si un servidor se identifica como comprometido, se puede aislar de la red para evitar más perjuicios a su organización. También se puede supervisar de forma precisa el tráfico y las aplicaciones del servidor, lo que permite priorizar aplicaciones importantes o denegar aplicaciones no deseadas.

A fin de facilitar el despliegue, se permite la instalación por script, lo que significa que el administrador del servidor puede dedicar su tiempo a otras tareas. Las listas blancas de aplicaciones con denegación por defecto, o control de aplicaciones basado en categorías, permite configurar más rápidamente lo que se permite y no se permite ejecutar en un servidor, en lugar de una configuración puramente manual.

Lista comparativa de productos

Después de leer las secciones anteriores para determinar sus requisitos básicos, utilice esta tabla para evaluar soluciones de distintos proveedores y establecer su idoneidad para su organización.

Comparación de funciones			Intercept X Advanced for Server with EDR	Trend Micro Deep Security	Symantec Protección de cargas de trabajo en la nube	Microsoft Enterprise Mobility + Security	CrowdStrike Falcon Prevent / Falcon Spotlight
GESTIÓN		Consola única para proteger servidores, endpoints, dispositivos móviles, correo electrónico y redes Wi-Fi	✓	×	×	×	×
		Detección de cargas de trabajo de AWS/Azure	✓	✓	✓	✓	✓
		Exclusiones de escaneado automáticas (por ejemplo, Exchange, SQL Server)	✓	×	✓	✓	×
		Virtualización: agente ligero con escáner centralizado	✓	✓	×	×	×
PREVENIR	REDUCIR SUPERFICIE DE ATAQUE	Filtrado web (bloquear sitios web maliciosos)	✓	✓	✓	✓	×
		Control web (controlar el acceso a sitios potencialmente inadecuados)	✓	×	×	×	×
		Listas blancas de aplicaciones (bloqueo de servidor)	✓	✓	×	✓	×
		Control de aplicaciones basado en categorías	✓	×	×	×	×
		Control de dispositivos/periféricos	✓	×	×	×	×
		Control de parches	×	✓	✓	✓	✓
	ANTES DE QUE SE EJECUTE	Protección contra malware con Machine Learning	✓	✓	✓	✓	✓
		Prevención de exploits	✓	✓	✓	✓	✓
		Prevención de pérdidas de datos	✓	×	×	✓	×
DETECTAR		Antihacker (p. ej., protección contra robos de credenciales y cuevas de código)	✓	×	×	✓	×
		Protección antiransomware (detección de comportamientos y reversión)	✓	✓	×	Detección, no reversión	Detección, no reversión
		Protección de disco y registro de arranque	✓	×	×	×	×
		Monitorización de integridad de archivos (FIM) / Monitorización de cambios	✓	✓	✓	✓	×
RESPONDER		Seguridad Sincronizada (integración inmediata con el firewall)	✓	×	×	×	×
		Visualización de la cadena de amenazas	✓	×	×	Requiere ATP de Defender	✓
		Búsqueda de amenazas	✓	×	×	Requiere ATP de Defender	✓

Seguridad centralizada

La protección de los servidores es una parte fundamental de la estrategia de seguridad de cualquier organización. Sin embargo, si tenemos en cuenta los otros dispositivos endpoint, teléfonos móviles, seguridad de redes, cifrado y demás factores, gestionar todo esto puede resultar difícil. De hecho, para muchos proveedores, cada una de las áreas de seguridad adicionales exige una consola y un marco de políticas adicionales, que suelen tener un aspecto y un funcionamiento diferentes y no ofrecen ninguna integración de la seguridad entre los distintos dispositivos y componentes de la infraestructura.

Sophos Central le permite gestionar todas sus soluciones de seguridad de Sophos desde una consola. Está diseñada para funcionar como un único panel intuitivo, con una interfaz de fácil uso y un aspecto uniforme entre los distintos productos. Y lo mejor de todo es que los productos de Sophos están creados para funcionar de forma conjunta, lo que le ofrece una mejor seguridad. Por ejemplo, sus servidores trabajan junto con sus firewalls para identificar, aislar y corregir automáticamente servidores comprometidos en cuestión de segundos.

Evaluación de la seguridad para servidores:

las 10 principales preguntas que hacer

Para evaluar una solución de protección para servidores, comience por hacer al proveedor las preguntas siguientes:

1. ¿Permite el producto distintos despliegues de los servidores, como localmente, en la nube e híbrido?
2. ¿Incluye el producto listas blancas de aplicaciones/denegación por defecto automatizadas sin costes adicionales?
3. ¿Tiene el producto tecnología específicamente diseñada para detener y revertir luego el ransomware?
4. ¿Qué tecnología existe para evitar los ataques sin archivos y basados en exploits? ¿Qué técnicas antiexploits se utilizan y qué tipos de ataques pueden detectar?
5. ¿Cómo protege el producto contra los ataques recurrentes por parte de adversarios activos?
6. ¿Qué técnicas utiliza el producto para detectar amenazas de malware desconocidas? ¿Utiliza el Machine Learning para buscar siempre atributos y comportamientos maliciosos?
7. Para los productos que dicen utilizar Machine Learning, ¿ha sido confirmada por un tercero la precisión de la detección? ¿Qué índices de falsos positivos ofrece?
8. ¿Qué visibilidad sobre los ataques ofrece el proveedor, como el análisis de causa raíz?
9. ¿Responde el producto automáticamente a las amenazas? ¿Puede limpiar una amenaza automáticamente en respuesta a un incidente?
10. ¿Se puede integrar el producto de forma nativa con la nube pública (p. ej., AWS/Azure/Google), incluida la capacidad de detectar automáticamente cargas de trabajo en la nube?

Conclusión

A medida que evolucionan las ciberamenazas tanto en complejidad como en virulencia, es sumamente importante tener implementada una protección efectiva en sus servidores. Entender las amenazas y las tecnologías de seguridad clave necesarias para detenerlas le permitirá elegir la mejor protección posible para los servidores de su organización. Y esta protección debe estar diseñada con las cargas de trabajo de los servidores en mente: no basta con ejecutar una protección para endpoints que no se ha adaptado a entornos de servidor.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

19-05-09 ES (PS)

SOPHOS