



Listas blancas de aplicaciones de servidores

Protección para servidores avanzada sin complicaciones.

Por **Tsailing Merrem**, director principal de marketing de productos

Los ataques sofisticados contra los servidores corporativos deben atajarse con un sistema de seguridad potente. El reto está en encontrar una solución que proporcione el nivel de protección adecuado y que, al mismo tiempo, pueda desplegarse y administrarse de forma eficiente y rentable. Las listas blancas de aplicaciones evitan que las amenazas avanzadas y desconocidas lleguen a los servidores, pero constituyen un sistema complejo y caro de desplegar. Sophos trae la potencia de las listas blancas de aplicaciones a los entornos empresariales a través de la nube, lo que las convierte en la solución por excelencia para proteger los servidores y los datos confidenciales que contienen.

El reto de proteger los servidores corporativos

El volumen y el valor de los datos almacenados en los servidores corporativos los han convertido en los principales objetivos del malware dirigido y de los ataques de día cero. La protección de la integridad y la disponibilidad de los servidores y de la confidencialidad de los datos que contienen es actualmente una de las grandes preocupaciones de cualquier organización. Hasta ahora, a las organizaciones no les quedaba más remedio que desplegar sistemas de seguridad en las estaciones de trabajo a fin de proteger los servidores. Sin embargo, la seguridad endpoint no distingue correctamente entre servidores y estaciones de trabajo, lo que requiere una configuración y una optimización extensivas y convirtiéndolo en un proceso sumamente complejo.

Las listas blancas de aplicaciones son cada vez más habituales en los entornos corporativos como el método más adecuado para evitar que las amenazas avanzadas y desconocidas lleguen a los servidores. Las listas blancas ayudan a las organizaciones a proteger el sistema operativo del servidor y las aplicaciones que instala con una regla de denegación por defecto, en lugar de centrarse en las amenazas conocidas (permitir por defecto). Este enfoque permite una protección sin firmas proactiva ante amenazas conocidas y desconocidas, y garantiza que solo las aplicaciones autorizadas por el departamento técnico se ejecuten en el sistema.

No obstante, las listas blancas de aplicaciones convencionales implican una enorme carga de administración, no solo en el momento del despliegue inicial, sino también durante el mantenimiento y la administración de cambios. A las empresas de tamaño mediano con conocimientos y recursos técnicos limitados se les suele desaconsejar la implementación de este método, o se les obliga a invertir en servicios de consultoría muy costosos.

Listas blancas de aplicaciones de Sophos— Una protección para servidores simple y efectiva

Sophos Server Protection constituye la solución de listas blancas de aplicaciones de servidor más sencilla para empresas medianas. Garantiza una seguridad efectiva, un rendimiento de los servidores optimizado, un despliegue rápido y una administración fácil. Se trata también de la única solución que ofrece listas blancas de aplicaciones totalmente integradas con sistemas HIPS (sistemas de prevención de intrusiones en el host) y antimalware para servidores para una protección efectiva ante ataques conocidos y de día cero, como los ataques en memoria, de inyección de DLL y basados en scripts.

Con la primera función de bloqueo del servidor con un solo clic del mercado, la solución escanea automáticamente el servidor en busca de malware al tiempo que marca las aplicaciones con huellas digitales, establece la línea de base de la lista blanca de aplicaciones y, a continuación, bloquea el servidor. Una vez en el modo de bloqueo, los archivos de las aplicaciones de línea de base no pueden reemplazarse ni manipularse. Sin embargo, Sophos Server Authority reconoce las aplicaciones del servidor y adapta su configuración para permitir automáticamente los cambios de confianza. Asimismo, establece las exclusiones de escaneo del antivirus de forma autónoma

DESCRIPCIÓN GENERAL

Las listas blancas de aplicaciones de Sophos, en combinación con los sistemas HIPS y antimalware avanzados, ofrecen una potente protección para servidores que es sencilla de desplegar y mantener.

ASEPECTOS DESTACADOS

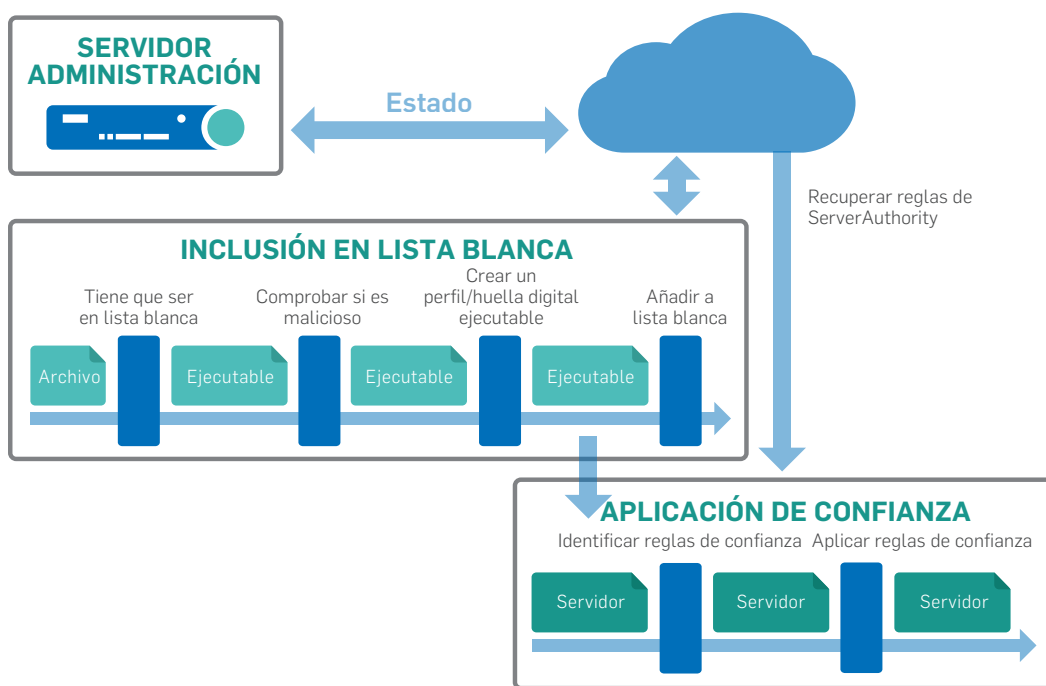
- ▶ Bloqueo del servidor con un clic
 - ▶ Reglas de confianza automáticas para adaptarse a un entorno de servidor
 - ▶ Integración con sistemas HIPS y antimalware para proteger contra ataques basados en contenidos y de día cero
 - ▶ Exclusiones de escaneo del antivirus automatizadas para mejorar el rendimiento
 - ▶ Protección y administración centralizada basadas en la nube
-

Listas blancas de aplicaciones de servidor

para un alto rendimiento. Estas funciones eliminan los procesos largos y tediosos que suponen las configuraciones y el establecimiento de reglas manuales. El motor de seguridad contextual de Sophos supervisa constantemente el sistema a fin de evitar los ataques basados en contenidos. Las listas blancas de aplicaciones con Sophos van más allá de las aplicaciones e incluyen también archivos DLL y scripts. Sophos Server Authority bloquea automáticamente la asociación entre las aplicaciones y sus archivos asociados, como archivos DLL y de script, para proteger el sistema de ataques basados en la memoria. Realiza todos estos procesos sin necesidad de reglas personalizadas, lo que evita la posibilidad de que se produzcan errores de configuración.

La solución está diseñada para maximizar el rendimiento de las aplicaciones del servidor. Proporciona alertas e informes personalizables que son accesibles desde cualquier parte mediante la consola integrada de Sophos Central. La interfaz de administración cuenta con un "único panel transparente" que ofrece al administrador del servidor una visión integrada de todos los servidores, las aplicaciones y el estado de protección.

Funcionamiento de las listas blancas de aplicaciones de Sophos



Bloqueo del servidor con un clic

Las listas blancas de aplicaciones de Sophos permiten bloquear el servidor con un solo clic. Ya no tendrá que preocuparse de configurar servidores físicos, establecer configuraciones de políticas, crear inventarios de aplicaciones ni escribir reglas para la administración de cambios. Lo que anteriormente suponía días e incluso meses de arduo trabajo, ahora es solo cuestión de un clic. Ese único clic pone en marcha un completo escaneado del sistema en busca de malware, al tiempo que cataloga aplicaciones y establece relaciones de confianza entre aplicaciones, actualizadores y archivos del sistema.

Reglas de confianza automáticas con Server Authority

Sophos Server Protection se adapta dinámicamente al entorno del servidor con Sophos Server Authority. Identifica las aplicaciones incluidas en la lista blanca y aplica las reglas de confianza necesarias para garantizar que sólo las fuentes de confianza puedan actualizar las aplicaciones de la lista blanca. Esto no sólo protege la integridad de las aplicaciones, sino que también garantiza que se les apliquen actualizaciones y parches sin interrupciones.

Sophos Server Authority mantiene una lista de aplicaciones de servidor populares como Controlador de dominio, Exchange Server y SharePoint, y aplica automáticamente las exclusiones del antivirus para evitar archivos y directorios que podrían afectar al rendimiento y a la estabilidad.

Seguridad integrada

Al integrar las listas blancas de aplicaciones de Sophos con Sophos Server Antivirus, nos aseguramos de que sus servidores permanecen protegidos utilizando ambas tecnologías para responder a las diversas amenazas presentes en la actualidad. La solución también utiliza Live Protection, una conexión con SophosLabs basada en la nube, para buscar amenazas en tiempo real.

Protección avanzada diseñada para servidores

Sophos Server Protection establece una distinción clara entre las políticas del usuario y las políticas del servidor. La política del servidor predeterminada está optimizada para equilibrar el rendimiento y la protección en sistemas operativos de servidor. Las políticas pueden aplicarse a un único servidor, a un grupo definido por Active Directory, manualmente en la consola o a todo el entorno.

Conclusión

En la actualidad, la urgencia y el reto que conlleva la protección de los servidores corporativos ante ataques conocidos y de día cero están aumentando a un ritmo paralelo. Las listas blancas de aplicaciones de Sophos ofrecen una protección potente a la vez que sencilla que es única en el mercado. La solución incluye el bloqueo del servidor con un clic, Sophos Server Authority para habilitar las fuentes de cambios de confianza automáticos, y los sistemas HIPS y anti-malware integrados. Esto ofrece a las empresas una administración de fácil uso, un rendimiento optimizado y una protección efectiva para sus servidores.

Sophos Server Protection

Para obtener más información,
visite es.sophos.com/Servers.

Ventas en España

Teléfono: (+34) 913 756 756

Correo electrónico: comercialES@sophos.com

Oxford (Reino Unido) | Boston (EE. UU.)

© Copyright 2015. Sophos Ltd. Todos los derechos reservados.

Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido

Sophos es la marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

04-16/NP.wpes