GUÍA DE COMPARACIÓN

Akamai Guardicore Segmentation frente a las soluciones de microsegmentación tradicionales

Visibilidad inigualable

Para comprender qué sucede en su entorno, es esencial tener visibilidad de las comunicaciones entre cargas de trabajo. Una visibilidad realmente eficaz significa poder saber en cualquier momento lo que está haciendo cada carga de trabajo con un contexto completo. Además, las capacidades de agrupación y filtrado de activos y reglas son componentes esenciales para crear políticas de forma rápida y eficaz.

Akamai	Microsegmentación tradicional
Visualice fácilmente todo el entorno El agente de Akamai Guardicore Segmentation es un firewall basado en host que se ejecuta en sistemas operativos tanto heredados como modernos, y que proporciona una visibilidad completa de los flujos de red al nivel de procesos y servicios individuales para los sistemas operativos Windows y Linux, así como para terminales MacOS.	**Visibilidad parcial en sistemas antiguos** No hay visibilidad en sistemas Microsoft Windows anteriores a Windows 2002. Esto se debe a que el agente de las soluciones de microsegmentación tradicionales se basa en el firewall de Windows, que solo estaba disponible en sistemas posteriores a 2002. Para los sistemas Linux, sus agentes solo admiten visibilidad hasta la capa 4.
Contexto enriquecido y sin igual Cuando se trata de visibilidad, es fundamental contar con el contexto y los detalles adecuados. Nuestra solución recopila, además de los datos de flujo, elementos críticos del contexto como la información del proceso, el archivo, el nivel en el que se han aplicado los parches, etc.	**Contexto mínimo** Recopila información solo de flujos y máquinas, sin detalles cruciales del contexto como el proceso y el archivo. Así es mucho más difícil entender las dependencias de las aplicaciones y se tarda más en hacerlo.
Ausencia de limitación en el tipo o número de etiquetas No imponemos restricciones en el número o tipo de etiquetas que puede tener, lo que permite una mayor flexibilidad y posibilita casos de uso adicionales. Esto le ahorrará el esfuerzo de tener que traducir las etiquetas existentes de las bases de datos de gestión de la configuración (CMDB) y otros orígenes de datos.	**Etiquetado rígido** Con una jerarquía de etiquetado fija y predefinida, las soluciones tradicionales le obligan a etiquetar sus aplicaciones utilizando solo una cantidad definida determinada por dichas soluciones, sin tener en cuenta los requisitos de su propio entorno y sus necesidades empresariales.
Etiquetado basado en IA La detección y el etiquetado de aplicaciones basados en IA le ayudarán a identificar las aplicaciones cuando no exista una CMDB fiable y les asignará la etiqueta correcta automáticamente.	**¿No tiene CMDB? Pues va listo…** Con el etiquetado manual y una jerarquía de etiquetas preconfigurada, si su organización no tiene una CMDB en la que confiar, el proceso de etiquetado se vuelve extremadamente complicado.

Akamai

Cobertura líder en el sector

Uno de los elementos principales de una buena solución de microsegmentación es la capacidad de proteger los activos esenciales, independientemente de dónde se implementen o dónde se acceda a ellos: sistemas antiguos y modernos, Windows o Linux, entornos locales o virtualizados, contenedores, etc.

Akamai

Compatibilidad total con Windows y Linux

Los agentes de Akamai Guardicore Segmentation son compatibles con todos los sistemas operativos Windows y Linux, tanto nuevos como antiguos, ya que nuestra solución no depende de la infraestructura subyacente.

Plena compatibilidad con contenedores

Visibilidad completa de los entornos contenedorizados al tiempo que se utilizan los controles de la interfaz de red de contenedores (CNI) para la aplicación.

Microsegmentación tradicional

Compatibilidad limitada con Windows y Linux

La aplicación de políticas depende del firewall de Windows para entornos Windows y de iptables para entornos Linux. Esto implica inevitablemente una protección limitada o nula para algunos sistemas operativos Windows antiguos, y la ausencia de reglas a nivel de procesos de capa 7 para entornos Linux.

Compatibilidad limitada con contenedores

La aplicación depende de iptables y cálculos de políticas repetidos que no se adaptan a un entorno de contenedor y que causan latencia y tiempo de inactividad.

Creación rápida de políticas sencillas

Un buen motor de políticas le permite expresar su intención utilizando el menor número posible de reglas, sin imponer restricciones al lenguaje de las políticas. También contribuirá a minimizar el trabajo de gestionar políticas mediante mecanismos de automatización y asistentes.

Akamai

Permiso y denegación

Admitimos las reglas de listas de autorización y denegación, y cualquier combinación intermedia. De esta manera, los equipos de seguridad y de respuesta a incidentes podrán responder rápido a cualquier situación, lo que elimina la necesidad de crear primero una lista de autorización para cada uno de los flujos legítimos.

Plantillas de políticas para una variedad de casos de uso

Plantillas listas para usar y flujos de trabajo de creación de políticas para los escenarios comunes: mitigación de ransomware, delimitación de aplicaciones, segmentación de entornos, etc. Con ellas, se puede ahorrar tiempo y reducir los errores humanos.

Amplia selección de criterios para políticas

Los criterios de las políticas pueden incluir el origen, el destino, el puerto, el protocolo, el proceso, el servicio (p. ej., el programador de tareas utilizado habitualmente por el ransomware), el usuario y el nombre de dominio completo (FQDN).

Microsegmentación tradicional

Lista de autorización cuya compatibilidad con las reglas de denegación es limitada

Seguir el modelo de lista de autorización, que es seguro pero requiere mucho tiempo, impide que las soluciones de segmentación tradicionales respondan automáticamente a las amenazas conocidas que exigen un bloqueo rápido.

Un conjunto limitado de plantillas

Las plantillas de segmentación se admiten principalmente en entornos de Microsoft. No se admiten plantillas para casos de uso de segmentación comunes, como la delimitación de aplicaciones y la mitigación del ransomware y resolución de los problemas que causa.

Criterios limitados

No hay políticas a nivel de procesos de capa 7 para sistemas operativos Linux ni capacidad alguna para crear políticas basadas en servicios individuales de Microsoft Windows.

La seguridad es lo primero

Luchar contra amenazas complejas, como el ransomware, requiere un enfoque integral de la seguridad. Aunque el Instituto Nacional de Normas y Tecnología (NIST) y la Casa Blanca prescriben la segmentación como una respuesta fundamental, este método requiere un enfoque integrado de la seguridad y la detección de filtraciones para mantener protegida su organización.

Akamai	Microsegmentación tradicional
Prevención y mitigación del ransomware Akamai Guardicore Segmentation proporciona plantillas listas para usar para todas las fases de la cadena de ataque, desde la prevención hasta la contención y la mitigación.	**Ausencia de plantillas ransomware** Las soluciones tradicionales tienen una capacidad limitada para bloquear ataques de ransomware con plantillas listas para usar.
Consulta de terminales para detectar amenazas y cumplir las normativas Nuestra herramienta Insight, basada en Osquery, permite consultar servidores y terminales en tiempo real para cumplir las normativas y detectar malware.	**Ausencia de detección en tiempo real** Las soluciones tradicionales no pueden detectar actividades maliciosas en tiempo real en el centro de datos.
Capacidades de engaño Basado en una tecnología patentada, el agente de Akamai Guardicore Segmentation redirige las sesiones bloqueadas y fallidas a un motor de engaño dinámico para su posterior análisis y puesta en cuarentena.	**Ausencia de sistema de puesta en cuarentena** Las soluciones tradicionales carecen de capacidades de engaño, así como de la capacidad de detectar o poner en cuarentena máquinas utilizando indicadores de riesgo (IOC) conocidos.
Equipo gestionado de búsqueda de amenazas Akamai proporciona servicios gestionados de búsqueda de amenazas que amplían las capacidades de su equipo de seguridad y permiten que su organización vaya siempre un paso por delante de las amenazas más recientes.	**Ausencia de servicios de búsqueda de amenazas** Los proveedores tradicionales no están en situación de prestar servicios de búsqueda de amenazas basados en su solución, lo que puede ser un gran factor diferenciador debido al incremento del ransomware y el malware.
Firewall de inteligencia ante amenazas Para evitar comportamientos malintencionados conocidos, Akamai Guardicore Segmentation bloquea IP, archivos y hash maliciosos mediante reglas de firewall automáticas.	**Sin fuentes de amenazas** Al carecer de una capacidad similar, las soluciones tradicionales no pueden detener el acceso a y desde direcciones IP y direcciones URL maliciosas conocidas.

Operaciones o rendimiento y latencia

La baja latencia es fundamental para que un proyecto de segmentación llegue a buen puerto. Esto significa que debe ser capaz de ampliar su política con más reglas, etiquetas por activos y otros elementos, todo ello sin aumentar la latencia.

Akamai

Motor optimizado para la latencia

Nuestro motor de segmentación está diseñado para escenarios a gran escala. Todo gracias a un mecanismo de filtrado optimizado que consigue que el tiempo de latencia sea relativamente insensible al tamaño de la política.

Microsegmentación tradicional

Un mayor número de reglas aumenta la latencia

Los agentes introducen más latencia a medida que aumenta la cantidad y el tamaño de las reglas. El software iptables de Linux no se diseñó para adaptarse al tráfico de este a oeste a nivel empresarial. El resultado es que la latencia aumenta significativamente a la par que el tamaño de la política.

Para obtener más información sobre Akamai Guardicore Segmentation o para solicitar una demostración personalizada del producto, visite akamai.com/guardicore.

 | Asistencia | Publicado en julio de 2023