INFORME SOBRE LA SOLUCIÓN DE AKAMAI

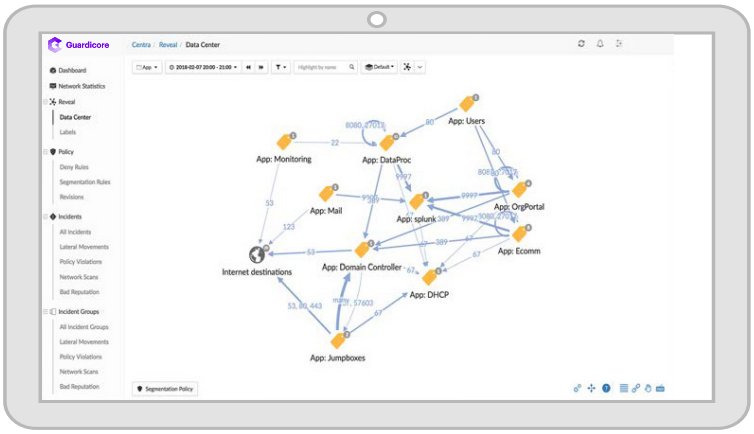
Microsegmentación rápida en entornos híbridos con Guardicore Segmentation de Akamai

El camino hacia la implementación de la microsegmentación no es una línea recta; hay muchos giros y vueltas a medida que comienza a descubrir, comprender y controlar los flujos de aplicaciones en su entorno de TI. Sin embargo, sin el enfoque adecuado para recorrer esta ruta, puede encontrarse con una serie de obstáculos a lo largo del camino. Los puntos ciegos de la red a menudo impiden detectar y asignar correctamente la comunicación entre las aplicaciones, las cargas de trabajo y los procesos subyacentes. Una aplicación incoherente de las políticas entre sistemas operativos puede dar lugar a peligrosas brechas de seguridad. La expresión incoherente de las políticas en los sistemas operativos puede dar lugar a peligrosas brechas de seguridad. Por último, las integraciones complejas (y a menudo manuales) de los datos de infracciones de políticas con herramientas de detección de filtraciones pueden ralentizar la investigación y la respuesta a incidentes. Guardicore Segmentation de Akamai le ayuda a recorrer con éxito el camino hacia la microsegmentación en tres pasos.

Paso 1: Detectar

Detecte aplicaciones y visualice flujos automáticamente

Guardicore Segmentation de Akamai ofrece una gran visibilidad, que permite detectar y visualizar automáticamente todas las aplicaciones, cargas de trabajo y flujos de comunicación con contexto en el nivel de proceso, independientemente de dónde residan. Tendrá la misma vista para los activos en el entorno local, en la nube, en varias nubes y mucho más. Esta visualización, junto con la importación automática de metadatos de orquestación, permite a los equipos de seguridad etiquetar y agrupar de forma rápida y sencilla todos los activos y aplicaciones, lo que optimiza el desarrollo de políticas.



Proteja las aplicaciones críticas dondequiera que residan

Independiente de plataformas

Guardicore Segmentation de Akamai puede visualizar activos y aplicar políticas de seguridad en todas las infraestructuras: en el entorno local, en la nube y en entornos multinube.

Rápida implementación de políticas

Las sugerencias de reglas automatizadas, un motor de políticas flexible y una interfaz de usuario intuitiva hacen que la creación y aplicación de políticas requieran menos tiempo.

Funciones integradas de detección y respuesta a filtraciones

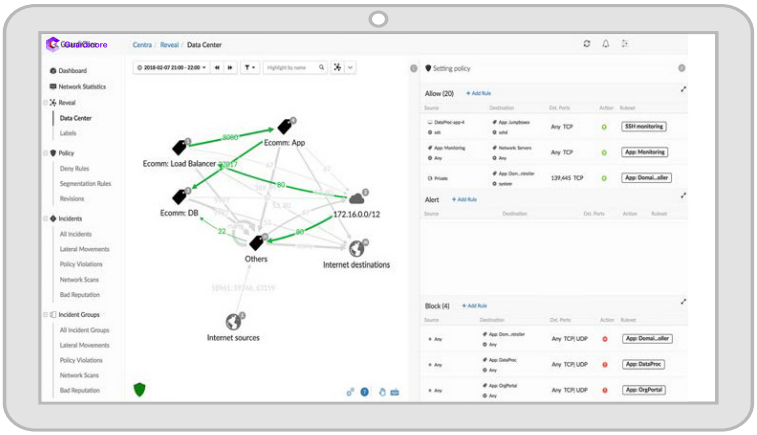
Visualice las infracciones de políticas y responda rápidamente a las amenazas activas para proteger sus activos críticos, independientemente de dónde residan.

Akamai

Paso 2: Construir

Diseñe, pruebe e implemente políticas rápidamente

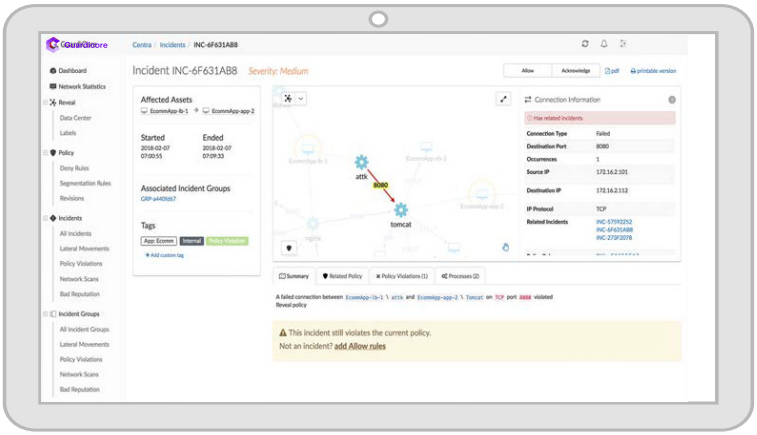
Guardicore Segmentation de Akamai simplifica el desarrollo y la gestión de políticas de microsegmentación. Basta con hacer clic en un flujo de comunicación en el mapa de detección para generar sugerencias de reglas automatizadas basadas en observaciones históricas, lo que le permite crear rápidamente una política sólida. Un flujo de trabajo intuitivo y un motor de políticas flexible permiten el perfeccionamiento continuo de las políticas y reducen los costosos errores.



Paso 3: Aplicar

Proporcione una seguridad sólida en cualquier entorno

Con la capacidad de aplicar políticas de comunicación en el nivel de red y de proceso en todos los sistemas, Guardicore Segmentation de Akamai garantiza la seguridad, independientemente de las limitaciones del sistema operativo. Además, las funciones integradas de detección y respuesta a filtraciones le permiten ver las infracciones de políticas en el contexto de una filtración activa, lo que le permite identificar rápidamente el método de ataque y corregirlo.



Visite akamai.com/guardicore para obtener más información.

 | Asistencia | | Publicado en 06/23