INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Protección de las cargas de trabajo en AWS con Akamai Guardicore Segmentation

Las empresas siguen aprovechando los recursos PaaS en Amazon Web Services (AWS) y muchas están migrando sus cargas de trabajo esenciales a la nube pública. Gracias a ello, están constatando algunas ventajas como la reducción de costes, la mejora de la escalabilidad y el rendimiento, y el aumento de la agilidad empresarial. Sin embargo, este cambio a la nube también plantea una serie de preocupaciones apremiantes en torno a la seguridad, entre las que se incluyen:

Nuevo conjunto de herramientas

Operar en un entorno de nube requiere un conjunto completamente nuevo de controles de seguridad. Estos controles deben ser compatibles con AWS en la nube y en el entorno local, a través de AWS Outposts, así como cargas de trabajo de nube híbrida. Los grupos de seguridad en la nube existentes pueden ser suficientes para los activos y recursos en la nube de AWS, pero esos controles no se extienden para proteger los activos o recursos relacionados en otros entornos. De esta forma, su equipo tiene que gestionar varias herramientas de seguridad, lo que puede dar lugar a posibles brechas en sus defensas.

Nuevo modelo de operaciones de seguridad

Como parte del modelo de responsabilidad compartida de AWS, el uso de recursos de AWS en la nube o de forma local implica que Amazon solo es responsable de proteger la infraestructura que ejecuta todos los servicios que se ofrecen en la nube de AWS. Sin embargo, cualquier software de aplicación o utilidades instaladas en esas instancias, así como la configuración de grupos de seguridad, son responsabilidad exclusiva del usuario. Esto también incluye la protección y supervisión del tráfico, tanto de norte a sur como de este a oeste, además de la implementación de controles para prevenir y detectar las posibles infracciones, así como para responder ante ellas.

Menor visibilidad y control de la infraestructura

Las mismas ventajas que hacen que el entorno de AWS sea atractivo desde el punto de vista operativo también pueden reducir el control y la visibilidad de los activos que se distribuyen entre varias cuentas de AWS, nubes privadas virtuales (VPC) y grupos de seguridad de red, así como el ecosistema híbrido más amplio de una organización.

Ventajas clave

- Solución integral para proteger las cargas de trabajo en AWS, como los recursos PaaS, lo que permite a los equipos de DevOps y seguridad centrar sus escasos recursos en las tareas principales en lugar de en la gestión de la seguridad del centro de datos.
- Gestione y aplique políticas de microsegmentación estrictas que se extienden más allá de AWS para incluir activos que residen de forma local e incluso en nubes públicas.
- Detecte de forma fiable las infracciones de políticas y responda a ellas en tiempo real.
- Proteja los entornos de posibles infracciones mediante varios métodos de detección y prevención de intrusiones, como análisis de reputación y sistemas de engaño dinámico en tiempo real.

Akamai Guardicore Segmentation para la seguridad de AWS

Akamai Guardicore Segmentation proporciona una solución unificada que garantiza la máxima visibilidad y la aplicación de las políticas para las cargas de trabajo y los recursos de PaaS que se ejecutan en la nube de AWS, en Outposts y en entornos híbridos. Proporciona microsegmentación y visibilidad a nivel de aplicación, así como capacidades de detección y respuesta ante infracciones.

Detección y visibilidad automáticas

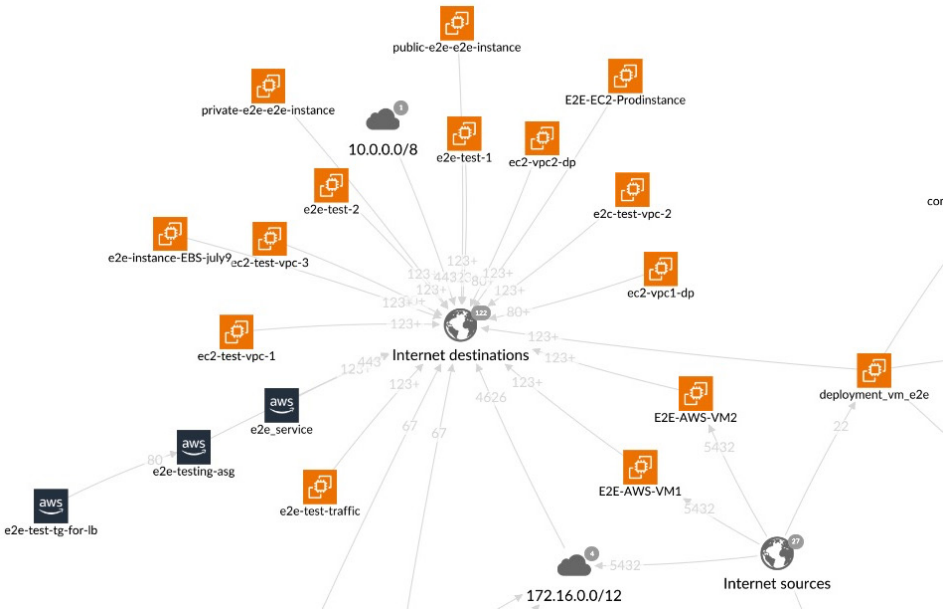
- Visualización automática de las aplicaciones, los recursos y sus flujos de comunicación
- Comprensión rápida y establecimiento de valores de referencia del comportamiento de las aplicaciones
- Asignación de dependencias de aplicaciones con visibilidad detallada hasta el nivel de proceso (capa 7)

Segmentación y aplicación eficaces

- Definición de políticas de segmentación en cuestión de minutos
- Recomendaciones automáticas de políticas
- Etiquetado y agrupación inteligentes que permiten una navegación sencilla por entornos complejos

Detección de amenazas y respuesta ante incidentes

- No es necesaria ninguna configuración; valor desde el primer día
- Varios métodos de detección para abordar todo tipo de amenazas
- Engaño dinámico para proporcionar una cobertura de red completa



Visualice y proteja las aplicaciones y los recursos en AWS con Akamai Guardicore Segmentation

> Con Akamai Guardicore Segmentation, pudimos abarcar las brechas de seguridad críticas de la microsegmentación y la visibilidad a nivel de aplicación, así como la detección y respuesta ante infracciones, cubriendo así tanto los servidores AWS como los del entorno local.
>
> — **Jefe de equipo de DevOps**
> Empresa de biotecnología

Proteja totalmente las cargas de trabajo y los recursos PaaS en AWS. Obtenga más información en akamai.com/guardicore.