Historia de cliente de Akamai

Una empresa de atención sanitaria de EE. UU venció 4000 ciberataques en un día

Los ingenieros de redes utilizaron la visibilidad de la capa 7 y políticas inteligentes mediante la microsegmentación para reducir los ciberriesgos

Ransomware frustrado | Mayor visibilidad | Mejores políticas

Conexión de los pacientes con la atención sanitaria esencial

Imagine tener que intentar proteger una red que afecta directamente a la vida de los pacientes y, al mismo tiempo, adelantarse a los ciberataques cada vez más sofisticados. Ese era el día a día para una empresa de atención sanitaria de tamaño medio. Su equipo de ingeniería de redes se enfrentaba a un número cada vez mayor de amenazas de ransomware y a la necesidad de tener una mayor visibilidad, por lo que recurrió a Akamai Guardicore Segmentation para mejorar la estrategia de seguridad de la empresa.

Ampliación de la arquitectura Zero Trust

La organización tenía una visión audaz: reforzar su entorno de TI con los principios de Zero Trust y, al mismo tiempo, cumplir con los requisitos de HIPAA y SOC 2. Dado que había mucho en juego, entre los objetivos del equipo de ingeniería de redes se incluían los siguientes:

- Mantener las aplicaciones críticas online incluso durante los incidentes de seguridad
- Reducir el impacto de los ataques de ransomware conteniendo su propagación
- Obtener una visibilidad detallada de la red mucho más amplia de la que ofrecen los firewalls tradicionales

La organización necesitaba una solución de microsegmentación rentable y escalable para la que no hiciera falta la eliminación y sustitución de la infraestructura de TI existente. Además, tenía que ser lo suficientemente fácil de usar como para que un equipo reducido la gestionara y lo suficientemente escalable como para crecer con la empresa.

Como explicó un ingeniero de redes, "El ransomware se dirige al sector de la atención sanitaria. Cuanto más rápido podamos aislar y eliminar estas amenazas, mejor".

Healthcare Company

Ubicación

Estados Unidos

Sector

Sanidad y ciencias de la vida

Solución

Akamai Guardicore Segmentation

Akamai

Búsqueda de la solución de microsegmentación adecuada

Después de descartar rápidamente la opción de un enfoque basado en contenedores, la empresa evaluó soluciones de microsegmentación. "Queríamos tener las mismas capacidades que vemos en los firewalls de última generación, a saber, visibilidad en la capa de aplicación", explicó el ingeniero de redes.

Después de evaluar muchas soluciones, la organización descubrió Akamai Guardicore Segmentation. Una demostración positiva combinada con la asistencia práctica de los ingenieros de Akamai cerraron el acuerdo. La solución satisface todas las necesidades, incluidas las siguientes:

- **Visibilidad integral:** inspección de capa 7 e información completa de la red
- **Facilidad de implementación:** agentes basados en software sin hardware adicional
- **Resiliencia:** sin ningún punto único de fallo en la red principal
- **Flexibilidad:** compatibilidad con diversos sistemas operativos

Según el vicepresidente de infraestructura de TI y seguridad de la información, Akamai Guardicore Segmentation ofrece una gran ventaja a los equipos reducidos. "Inmediatamente después de iniciar la implementación, obtuvimos beneficios en cuanto a la visibilidad y el control".

"No necesitamos comprar y gestionar varios firewalls este-oeste, lo que supone un enorme ahorro de costes, y también obtenemos un nivel de visibilidad que no es posible a través de los firewalls", añadió el responsable de la infraestructura de TI.

Detención del avance del ransomware

Los resultados fueron inmediatos e impresionantes. Gracias a una mejor delimitación de sus aplicaciones y al uso de las políticas de prevención de ransomware listas para usar de Akamai Guardicore Segmentation, el equipo neutralizó 4000 ciberataques el primer día. La solución incluso personalizó las políticas para adaptarse a las necesidades específicas de la organización.

"En el caso de las políticas de nivel intermedio, utilizamos el modo de alerta para marcar los incidentes sin causar tiempo de inactividad. Es una forma excelente de perfeccionar las políticas sin interrupciones", compartió el ingeniero de redes.

> Akamai Guardicore Segmentation no solo acabó con nuestras preocupaciones sobre el ransomware, sino que mejoró nuestro enfoque con respecto a la ciberseguridad.
>
> **– Ingeniero de redes**

> "Comenzar a gestionar el enfoque Zero Trust es un desafío increíble. Akamai Guardicore Segmentation nos ayudó a dominar rápidamente el enfoque, al mismo tiempo que reducía los problemas de complejidad y costes".
>
> — Vicepresidente de infraestructura de TI y seguridad de la información

Obtención de información sin precedentes sobre la capa 7

Según el director de infraestructura de TI, Akamai Guardicore Segmentation proporciona vistas valiosas de los flujos de tráfico entre diferentes aplicaciones. Esto descubrió una valiosa fuente de datos para el equipo. El equipo ahora podía inspeccionar detalles muy precisos más allá de los registros de capa 4: los ID de usuario, las entradas de línea de comandos e incluso las correlaciones entre servicios.

"Nuestro equipo de red puede examinar el flujo de tráfico para solucionar problemas y proporcionar a nuestro equipo de seguridad la información necesaria para investigar los incidentes en profundidad", señaló el ingeniero de red.

Esta visibilidad resultó útil durante una infracción inesperada de las políticas. Un nuevo empleado conectó un PC directamente al equipo de las instalaciones del cliente (CPE) de su operador en lugar de a un puerto LAN protegido por un router interno. Esto fue un error enorme, ya que el CPE asignó al PC una IP pública, haciéndolo susceptible a los escaneos públicos de Internet.

Como explicó el ingeniero de red de la organización, "Akamai Guardicore Segmentation detectó el problema al instante, lo que nos permitió aislar el PC y resolver la situación antes de que la amenaza se materializara. Además, esto nos inspiró a crear una política diseñada para evitar que este tipo de incidentes ocurra en el futuro".

Etiquetado más inteligente y mejores políticas

Gracias al etiquetado intuitivo y a la creación de políticas, el equipo de ingeniería de redes pudo asignar fácilmente el tráfico y aplicar reglas de seguridad. Como dice el ingeniero de redes: "Podíamos decidir qué funciona mejor para nuestro entorno. Esa capacidad nos impresionó mucho más de lo que esperábamos y nos ayudó a crear políticas de manera eficiente".

Por ejemplo, el equipo limitó el acceso a los servidores de impresión permitiendo solo zonas de confianza, una ventaja rápida que mejoró la estrategia de seguridad general de la organización. "Eso nos permitió implementar las correcciones más ventajosas desde el principio", continuó el ingeniero.

Visibilidad que infunde confianza

¿Cuál fue uno de los beneficios inesperados? Una visión clara del flujo de tráfico interno y del comportamiento de las aplicaciones. Esta nueva visibilidad sirvió para mejorar la colaboración con los propietarios de las aplicaciones y optimizar los plazos de mantenimiento. Por ejemplo, el equipo está capacitado para mostrar a los propietarios de las aplicaciones si su tráfico está bloqueado.

"En el pasado, la solución de problemas y la preparación para el futuro eran un problema. Ahora, durante las transiciones, podíamos confirmar con confianza cuándo cambiaba el tráfico de los servidores antiguos a los nuevos. Eso nos permitió retirar los sistemas heredados con total confianza", dijo el ingeniero de redes.

El vicepresidente de infraestructura de TI y seguridad de la información de la organización concluyó: "Akamai Guardicore Segmentation ya ha marcado la diferencia y se ha convertido en un producto esencial en nuestras prácticas de seguridad. Espero con ganas el momento de extender su implementación a toda la organización".

| Publicado en febrero de 2025