

HISTORIA DE CLIENTE DE AKAMAI

Un importante sistema sanitario selecciona Akamai para mejorar la estrategia de conformidad normativa y permitir la migración a la nube



Visibilidad completa de la red



Segmentación en todas las infraestructuras de TI



Adopción segura de nuevas tecnologías

Resumen del cliente

Como importante sistema sanitario, este cliente de Akamai es responsable de proteger sus más de 6000 activos y los datos de los pacientes frente a posibles amenazas.

Desafíos o requisitos empresariales

Aunque la organización tenía previsto migrar algunas de sus cargas de trabajo esenciales a Microsoft Azure, sus responsables de TI se tuvieron que enfrentar a una serie de obstáculos para conseguir que la adopción de la nube se llevara a cabo con éxito.

Su entorno actual presentaba varios riesgos de seguridad, entre los que se incluían una red relativamente plana en la que los dispositivos de Internet de las cosas médicas tenían acceso sin supervisión al centro de datos y una política "traiga su propio dispositivo" (BYOD) muy aprovechada. Esto suponía que una posible filtración podía dar lugar a una propagación lateral y poner en peligro los datos de pacientes y pagos en otras aplicaciones esenciales. Con un aislamiento mínimo, dar prueba de cumplimiento a los auditores se convertía en una tarea manual que exigía una revisión exhaustiva de los registros de seguridad.

Igualmente frustrante era la falta de visibilidad del tráfico y de las dependencias de las aplicaciones que obstaculizaba los intentos de migrar las cargas de trabajo a Azure.

¿Por qué Akamai?

Afrontar los desafíos actuales de visibilidad y seguridad de la organización mediante VLAN o firewalls habría supuesto una coordinación y un esfuerzo considerable de los distintos equipos, ya al límite, para aplicar los cambios de red necesarios.

Por lo tanto, cuando el equipo de Akamai pudo demostrar un enfoque de segmentación definido por software capaz de representar de forma detallada su complejo entorno, así como aplicar políticas de segmentación de forma sistemática a las cargas de trabajo a nivel local y en la nube, las partes interesadas cerraron el presupuesto, mientras que los responsables de TI acabaron tomando una decisión de compra.



Sector

Atención sanitaria

Solución

[Guardicore Segmentation de Akamai](#)

Resultados clave

- Previene el movimiento lateral no autorizado
- Protege las aplicaciones críticas
- Simplifica y acelera la conformidad
- Migración segura a la nube



Resultados de Akamai Guardicore Segmentation

Simplificación y aceleración de la microsegmentación

Dado que Akamai Guardicore Segmentation utiliza un enfoque basado en software que es independiente de la infraestructura subyacente, el equipo de seguridad del cliente pudo acelerar el proyecto de segmentación por separado, lo que limitó el impacto en otros grupos de TI.

Con la nueva plataforma, la organización pudo acordonar rápidamente las aplicaciones esenciales y restringir de forma estricta el acceso de los dispositivos al centro de datos, todo ello sin tiempo de inactividad y sin necesidad de hacer cambios en las aplicaciones o en la red. Gracias a la nueva visibilidad de los datos históricos y en tiempo real, la organización también puede demostrar fácilmente a los auditores que todos los activos regulados están aislados de forma eficaz. Actualmente, son solo dos empleados los que se encargan de gestionar la seguridad del centro de datos de la empresa.

Por último, al asignar las dependencias de las aplicaciones y crear las políticas necesarias, el sistema sanitario logró alcanzar sus objetivos de adopción de la nube y garantizar, al mismo tiempo, que cualquier futura migración de cargas de trabajo a la nube siguiera siendo igual de segura.

Visite akamai.com/guardicore para obtener más información.



Es importante poner a los clientes potenciales de servicios de salud frente a la solución [Akamai] para que puedan ver todo el tráfico del centro de datos desde una única perspectiva y comprobar lo fácil que es crear y aplicar políticas de seguridad en entornos de nube híbrida.

— Responsable de seguridad de TI de un importante sistema sanitario