INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Informática confidencial: Protección de los datos en uso

A pesar de que el alcance, la escala y la sofisticación de las amenazas no paran de aumentar, los equipos de seguridad normalmente son capaces de hacer frente al desafío, especialmente cuando se trata de cifrar los datos durante su transferencia y limitar el acceso durante su almacenamiento. Sin embargo, cada vez se hace más evidente que los equipos también necesitan proteger los datos mientras se editan, leen o procesan activamente, a lo que se suele hacer referencia como *datos en uso*.

Esta brecha en la protección de los datos en uso es cada vez más importante en un contexto de evolución de la informática y auge de la inteligencia artificial (IA). La prevalencia de la informática híbrida y multinube ha aumentado los métodos con que las organizaciones recopilan y almacenan los datos. Al mismo tiempo, y a medida que tratan de sacar partido de la IA, las organizaciones utilizan conjuntos de datos enormes, que a menudo incluyen sus datos más valiosos y confidenciales, sin cifrar ni proteger.

Estos riesgos están avivando el interés en la informática confidencial, enfoque de seguridad que garantiza que los datos confidenciales que utilizan las aplicaciones, los procesos o los servicios permanezcan cifrados y protegidos.

Las API añaden complejidad

Las API están proliferando porque desempeñan funciones esenciales en dos áreas en las que las empresas dedican recursos de forma continua: los entornos y servicios en la nube, así como los modelos de IA. En la nube, las API resultan esenciales para que las tecnologías se puedan comunicar y compartir datos. Con la IA, los modelos de lenguaje de gran tamaño (LLM) utilizan API para acceder a los datos y combinarlos con el fin de llevar a cabo tareas complejas como la comprensión del lenguaje y la generación de textos.

Lamentablemente, los equipos de seguridad no prestan la misma atención a las API que a las aplicaciones y a la infraestructura. Los atacantes aprovechan esta vulnerabilidad, que ha llevado a que un 84 % de las organizaciones haya sufrido incidentes de seguridad relacionados con las API en los últimos 12 meses.[1] Para proteger los datos confidenciales que se usan en cada una de sus API relacionadas con la nube y la IA, las empresas necesitan funciones de seguridad de API integrales que protejan sus entornos informáticos confidenciales.

Bloqueo de las tres puertas

Aunque se bloquee el acceso a los datos en tránsito y almacenados, puede quedar una puerta totalmente abierta (la de los datos en uso), que expone a las empresas a riesgos.

En la informática confidencial, esos datos se procesan en un entorno que se considera fiable a nivel de hardware. Con las API, las organizaciones pueden implementar sus propias instancias privadas de aprendizaje automático (ML), diseñadas específicamente para proteger el tráfico de las API en lugar de utilizar un servicio de API de nube pública, lo que reduce drásticamente su superficie de ataque. El uso de una solución para proteger las API en un entorno informático confidencial añade una capa adicional de seguridad. Incluso aunque una parte del sistema se haya visto afectada por un ataque, los datos del entorno protegido permanecen seguros. Los análisis de las API de estos datos en un entorno de confianza se lleva a cabo de forma más segura, además de eliminar el riesgo existente en los entornos tradicionales.

Esta combinación de IA, seguridad de las API e informática confidencial permite evitar que entidades no autorizadas, como el hipervisor, el propietario de la infraestructura del sistema host o cualquier persona con acceso físico, vean o cambien el código o los

Ventajas para la empresa

Seguridad de datos mejorada
Limite el acceso a los datos en uso con estrictos controles, con el fin de reducir la superficie de ataque y proteger los procesos confidenciales basados en API frente al acceso no autorizado.

Protección de las API
Ejecute un análisis exhaustivo del tráfico de las API mientras mantiene cifrados los datos confidenciales en uso, lo que permite reducir el riesgo de exposición durante la supervisión.

Mejor cumplimiento de las normativas
Cumpla las estrictas normativas de protección de datos globales en constante cambio, garantizando que se respeten los estándares gubernamentales y del sector.

1. Akamai, Estudio sobre el impacto de la seguridad de API de 2024

datos durante la ejecución. De esta forma, se ofrece protección contra amenazas internas (por ejemplo, administradores de sistemas no autorizados o cargas de trabajo que se ejecutan en una infraestructura no fiable) y externas (por ejemplo, atacantes que aprovechan las vulnerabilidades).

Ventajas

En un entorno en el que proliferan las amenazas a las API y los datos en uso se convierten en un blanco atractivo, no es de extrañar que los atacantes merodeen. Las organizaciones con visión de futuro están empezando a adoptar la informática confidencial por varios motivos:

- En primer lugar, limitar el acceso a los datos en uso mediante sólidos controles.
- Analizar de forma segura el creciente número de API.
- Ajustarse a los nuevos y estrictos requisitos de cumplimiento de las normativas sobre protección de datos en todo el mundo con los controles que ofrece la informática confidencial.

La informática confidencial está especialmente indicada para las empresas muy reguladas, ya hablemos de una empresa de servicios financieros que desee proteger las transacciones online o de una empresa de ciencias de la vida que protege los datos de sus pacientes. Este enfoque también puede ayudar a un proveedor de software independiente a proteger un modelo de IA que distribuya a sus clientes de distintas ubicaciones, desde el Edge hasta la nube. De hecho, cualquier división de TI que haga análisis en tiempo real de sus datos esenciales debe plantearse el uso de la informática confidencial.

Cómo podemos ayudar nosotros y nuestros partners

Para ser eficaz, la informática confidencial debe contar con un conjunto integrado de soluciones que interactúen perfectamente para proporcionar un control y una protección totales. Akamai, junto con sus partners Intel e IBM, garantiza la seguridad de los datos en uso desde el nivel de hardware, pasando por la nube y hasta las API.

En primer lugar, Intel® Trust Domain Extensions (TDX) proporciona entornos de ejecución fiables que:

- Ofrecen protección frente a intrusiones externas de atacantes o entidades no maliciosas que no deberían tener acceso.
- Mejoran la seguridad del software que controla la tecnología utilizada para crear recursos virtuales en la nube, como redes, servidores y almacenamiento.
- Añaden una capa de seguridad muy necesaria para que las personas que administran cualquiera de estos sistemas distribuidos puedan reducir el riesgo de errores de buena fe y posibles casos de actividad malintencionada a nivel interno.

Además, la verificación y los tokens de Intel Tiber™ Trust Authority permiten a las organizaciones limitar y controlar el acceso a los datos en uso no cifrados.

Akamai API Security proporciona un inventario de las API utilizadas en la empresa y, a continuación, supervisa y detecta cómo se utilizan estas. La solución identifica y bloquea automáticamente las solicitudes de API maliciosas mediante el análisis de patrones y comportamientos de tráfico, neutralizando las amenazas en el Edge de la red sin necesidad de intervención manual. De esta forma, es posible protegerse en tiempo real de los ataques a las API, como filtraciones de datos, acceso no autorizado y abuso de la lógica.

Los motores de aprendizaje automático remoto de Akamai, junto con los procesadores Intel Xeon® en servidores de IBM Cloud Virtual Server, que a su vez están protegidos con Intel TDX y avalados por Intel Tiber Trust Authority, ofrecen un entorno privado e hiperescalable diseñado para evitar que cualquier amenaza externa acceda a los datos cuando se descifran durante la fase final de los datos en uso, ya se trate de ataques de bots basados en IA o de atacantes humanos.

Ha llegado el momento de proteger los datos en uso

Las organizaciones necesitan un entorno de gran confianza para proteger sus datos corporativos más valiosos, no solo cuando se almacenen o se acceda a ellos, sino cuando realmente se utilicen. Ese es el motivo por el que recurren a Akamai y a nuestros partners para disfrutar de una seguridad integral. Juntos, estos nombres consolidados en la informática garantizan la seguridad de los datos en cada etapa de su ciclo de vida.

Obtenga más información sobre cómo nuestra colaboración para ofrecer informática confidencial puede ayudarle a proteger sus datos más sensibles.
Obtenga más información sobre la solución Akamai API Security.