Historia de cliente

# Zero Trust avanzado de Cocamar con Akamai

La cooperativa agrícola Cocamar obtiene visibilidad, reduce el ciberriesgo y consigue un programa de seguridad más maduro

Visibilidad más completa del riesgo

Reducción del riesgo de carga de ransomware en un 93 %

Mejora de la madurez de la seguridad

## Mejora de operaciones digitales seguras en agricultura

Cocamar Agroindustrial Cooperative depende de la tecnología para mantener en marcha sus operaciones agrícolas. Estas operaciones abarcan desde la recepción de las cosechas hasta la gestión de las finanzas, la fabricación y la logística. A medida que la cooperativa ampliaba sus servicios digitales, necesitaba una mayor visibilidad de los crecientes ciberriesgos y una mayor protección para sus sistemas esenciales. En colaboración con Akamai, Cocamar ha sustituido una seguridad basada en hardware limitada por una seguridad de aplicaciones distribuida en la nube, protección contra **bots** y **microsegmentación**. El resultado ha sido una mayor visibilidad, una respuesta más rápida y un aumento significativo de la madurez general de la seguridad de la organización.

## La tecnología mantiene a la cooperativa en marcha

Fundada en 1963, Cocamar Agroindustrial Cooperative apoya a más de 20 000 familias agrícolas en todo Brasil. Cada etapa de su negocio depende de la tecnología, desde aceptar las entregas de cereal hasta emitir recibos.

"Nuestras operaciones están muy automatizadas", explica Paula Rebelo, directora ejecutiva de TI de Cocamar Agroindustrial Cooperative. "La tecnología acelera el negocio, pero también aumenta la importancia de la seguridad de la información".

A medida que Cocamar se expandía tanto geográfica como financieramente, su transformación digital se aceleró. Las nuevas aplicaciones, API e integraciones ayudaron a respaldar ese crecimiento. Pero también aumentó el potencial de ciberriesgos, incluidas las brechas y los accesos no autorizados.

La importancia de proteger los sistemas de Cocamar es especialmente evidente durante la temporada de cosecha. Cuando los agricultores entregan el maíz o la soja, los sistemas automatizados reciben cada envío, clasifican las cosechas y emiten los recibos en cuestión de minutos. Cualquier interrupción puede retrasar las operaciones y afectar a la confianza que los miembros de la cooperativa depositan en la organización.

"No podemos arriesgarnos a cerrar una planta o retrasar un envío debido a una brecha de seguridad", afirma Paula.

cocamar

**Ubicación**
Maringá, Brasil
cocamar.com.br

**Sector**
Fabricación

**Solución**
Seguridad

**Productos**
Akamai Guardicore Segmentation
App & API Protector
Bot Manager

Akamai Security

A medida que Cocamar continuaba añadiendo servicios digitales, cada nueva conexión creaba otro punto de entrada potencial para los atacantes. El equipo de seguridad sabía que necesitaba una mayor protección antes de que esos riesgos se convirtieran en problemas empresariales.

## Obtener visibilidad de los crecientes ciberriesgos

Cocamar comenzó a modernizar sus operaciones en 2021. En ese momento, protegía las aplicaciones orientadas a Internet con un **firewall de aplicaciones web (WAF)** basado en hardware. Aunque es eficaz para una protección básica, la plataforma ofrece poca visibilidad de las amenazas modernas y requiere una inversión continua en infraestructura física.

"Nuestra principal prioridad era ganar visibilidad de los riesgos a los que nos enfrentábamos", comenta Paula. "Teníamos muchas integraciones, API y portales, pero no podíamos ver claramente los riesgos que se introducían".

El equipo de seguridad evaluó a varios proveedores, incluidos AWS e Imperva. Después de numerosas pruebas de concepto, Akamai **App & API Protector** destacó tanto por sus capacidades como por la asistencia proporcionada por el partner local CPD.

"Akamai demostró ser la mejor opción para nosotros", añade. "Durante la prueba de concepto, ganamos una visibilidad que nunca antes habíamos tenido".

App & API Protector, una solución integral de protección de API y aplicaciones web, ayudó al equipo a realizar un descubrimiento sorprendente. Las aplicaciones que creía que estaban bien protegidas corrían un gran riesgo. "Antes, mi equipo estaba a ciegas. Con Akamai, finalmente fuimos conscientes del nivel de actividad de bots y de los intentos de ataque dirigidos a nuestras aplicaciones", explica.

La migración también eliminó las limitaciones de los dispositivos de hardware. "Con nuestro WAF físico, estábamos limitados por la infraestructura", añade Paula Rebelo. "Después de pasar a Akamai, obtuvimos una mejor visibilidad y ya no teníamos esas limitaciones. Ahora mi equipo puede tomar medidas rápidamente".

## Detener los bots maliciosos sin ralentizar el negocio

Tras obtener visibilidad del volumen de ataques automatizados dirigidos a sus aplicaciones, Cocamar dio el siguiente paso con la implementación de Akamai **Bot Manager**. La solución detecta y bloquea los bots maliciosos en el Edge, al tiempo que permite a los usuarios legítimos y a los bots de confianza acceder a las aplicaciones sin interrupciones.

"Ahora tenemos una herramienta que identifica los intentos de acceso no autorizados, como los bots maliciosos que intentan penetrar en nuestra red o en nuestras aplicaciones", señala Paula. "La solución nos permite automatizar el control del tráfico y limitar el acceso".

La actividad de bots fluctúa a lo largo del año, especialmente a medida que cambian los servicios digitales y las operaciones estacionales de la cooperativa. En lugar de ajustar constantemente las defensas, el equipo de seguridad puede confiar en Bot Manager para adaptarse automáticamente a la demanda.

"El número de bots que vemos varía de un mes a otro", explica. "Un mes, Bot Manager podía bloquear 100 000 bots y otro mes 200 000. Saber que tenemos una solución que puede gestionar cualquier volumen nos da la confianza de que nuestro entorno es seguro mientras los usuarios legítimos continúan accediendo a nuestras aplicaciones".

> **Akamai se convirtió en un partner esencial a la hora de mejorar nuestra madurez en seguridad de la información.**
>
> **Paula Rebelo**
> **Directora ejecutiva de TI, Cocamar Agroindustrial Cooperative**

## Contener las amenazas mediante la microsegmentación

Aunque App & API Protector y Bot Manager reforzaron las defensas de Cocamar en Internet, el equipo de seguridad también quería proteger mejor sus sistemas internos esenciales. Esto llevó a la cooperativa a implementar **Akamai Guardicore Segmentation** para controlar el acceso entre servidores y limitar hasta dónde podría un atacante moverse dentro del entorno.

"Nuestro objetivo era evitar el acceso no autorizado a nuestros servidores", explica Paula. "La microsegmentación nos ayuda a determinar quién debe tener acceso a qué y solo cuando lo necesite. "No hay un administrador con acceso a todo".

La máxima prioridad era proteger el sistema ERP (planificación de recursos empresariales) interno de Cocamar y el sistema operativo Oracle Solaris que hay detrás. Juntos, administran las finanzas, los recursos humanos, la fabricación y las operaciones diarias de la cooperativa.

"Ese entorno es el centro de nuestras operaciones", comenta Paula Rebelo. "Protegerlo frente a accesos no autorizados era una de nuestras mayores preocupaciones".

Durante la prueba de concepto, Akamai Guardicore Segmentation descubrió rutas de comunicación que el equipo no sabía que existían. Los servidores que debían haberse aislado intercambiaban tráfico, lo que los exponía a riesgos innecesarios. "La prueba de concepto nos mostró que estábamos a ciegas con respecto a ciertas comunicaciones entre servidores", apunta Paula.

La visibilidad proporcionada por Akamai Guardicore Segmentation permitió al equipo reforzar las políticas, reducir la comunicación innecesaria entre sistemas y protegerse mejor contra el movimiento lateral si un atacante obtenía acceso.

"Antes, no podíamos ver claramente cómo se comunicaban nuestros servidores en segundo plano. Ahora podemos identificar conexiones innecesarias y segmentar rápidamente el entorno para reducir el riesgo", añade.

La implementación también reforzó el programa de seguridad más amplio de Cocamar al integrarse con sus herramientas de gestión de vulnerabilidades. Cuando los análisis de vulnerabilidades identifican sistemas de alto riesgo, Akamai Guardicore Segmentation puede restringir inmediatamente la comunicación entre los servidores afectados, lo que ayuda a reducir la exposición mientras se está realizando la corrección.

A medida que crecía la confianza en la plataforma, Cocamar amplió la implementación, pasando de proteger 15 servidores a proteger más de 200. Trasladó las políticas esenciales de la solución al modo de bloques, utilizó la delimitación para aislar los activos esenciales e implementó la microsegmentación a nivel de servicio siempre que era posible.

El equipo también utiliza la solución para demostrar la reducción de ciberriesgos a su comité de seguridad de la información multidisciplinar. "Presentamos los riesgos y los escenarios simulados al comité", señala Paula. "En determinados escenarios, hemos demostrado que el uso de Akamai Guardicore Segmentation reduce el riesgo de carga útil de **ransomware** en un 93 %".

## Crear una cultura de la seguridad más sólida

Cada implementación de Akamai revelaba riesgos que Cocamar no sabía que existían. App & API Protector desveló los riesgos ocultos de las aplicaciones y la actividad de los bots. Bot Manager cuantificó y controló la automatización maliciosa. Akamai Guardicore Segmentation sacó a la luz comunicaciones de servidor inesperadas, un acceso con exceso de permisos y oportunidades de reducir el movimiento lateral.

Combinada, toda esta información ayudó a Cocamar a pasar de reaccionar a las amenazas a gestionar de forma proactiva los ciberriesgos. La cooperativa obtuvo mayor visibilidad y capacidades de respuesta más rápidas. Estas mejoras permitieron un programa de seguridad más maduro que continúa protegiendo sus operaciones esenciales. "Akamai hizo que nuestro entorno fuera más seguro, más fácil de gestionar y con menos riesgos", afirma Paula Rebelo.

Para Paula, Akamai se ha convertido en algo más que un proveedor de tecnología. "Akamai es un gran partner, no solo en cuanto a herramientas, sino también a lo largo de nuestro camino hacia la creación de una cultura de seguridad más sólida. La madurez de nuestra seguridad de la información se encuentra en un nivel completamente nuevo, gracias a las herramientas de Akamai", concluye Paula.

cocamar

Fundada en 1963 como Cooperativa de Cafeicultores de Maringá Ltda, Cocamar Agroindustrial Cooperative reunió inicialmente a un grupo de 46 fundadores, todos ellos productores de café, para organizar la producción regional y para recibir y procesar el producto. Hoy en día, se encuentra entre las cooperativas más grandes de Brasil y posee el complejo industrial más grande y diversificado dentro del sector cooperativo brasileño. Cocamar opera en 100 instalaciones en municipios del norte y noroeste de Paraná, oeste de São Paulo y suroeste de Mato Grosso do Sul, con aproximadamente 14 000 productores dedicados al cultivo de soja, maíz, trigo, café y naranjas.

© 2026 Akamai Technologies | Asistencia |
| Publicado en octubre de 2026