Customer Story

Cocamar Advanced Zero Trust with Akamai

Agricultural cooperative Cocamar gained visibility, reduced cyber risk, and enabled a more mature security program

Gained complete risk visibility

Cut ransomware payload risk by 93%

Improved security maturity

Improving secure digital operations across agriculture

Cocamar Agroindustrial Cooperative depends on technology to keep its agricultural operations moving. Those operations span everything from receiving crops during harvest to managing finance, manufacturing, and logistics. As the cooperative expanded its digital services, it needed better visibility into growing cyber risks and stronger protection for its most critical systems. Working with Akamai, Cocamar replaced limited, hardware-based security with cloud-delivered application security, **bot** protection, and **microsegmentation**. The result was greater visibility, faster response, and a significant increase in the organization's overall security maturity.

Technology keeps the cooperative running

Founded in 1963, Cocamar Agroindustrial Cooperative supports more than 20,000 farming families across Brazil. Every stage of its business depends on technology, from accepting grain deliveries to issuing receipts.

"Our operations are highly automated," explained Paula Rebelo, Executive Manager of IT of Cocamar Agroindustrial Cooperative. "Technology speeds up the business, but it also increases the importance of information security."

As Cocamar expanded both geographically and financially, its digital transformation accelerated. New applications, APIs, and integrations helped support that growth. But it also increased the potential for cyber risks, including breaches and unauthorized access.

The importance of protecting Cocamar's systems is especially clear during harvest season. When farmers deliver corn or soybeans, automated systems receive each shipment, classify the crop, and issue receipts within minutes. Any disruption can delay operations and affect the confidence that cooperative members place in the organization.

"We can't risk shutting down a plant or delaying a shipment because of a security breach," Rebelo said.

As Cocamar continued adding digital services, every new connection created another potential entry point for attackers. The security team knew it needed stronger protection before those risks became business problems.

cocamar

Location
Maringá, Brazil
cocamar.com.br

Industry
Manufacturing

Solution
Security

Products
Akamai Guardicore Segmentation
App & API Protector
Bot Manager

Akamai Security

Gaining visibility into growing cyber risks

Cocamar began modernizing its operations in 2021. At the time, it protected internet-facing applications with a hardware-based **web application firewall (WAF)**. While effective for basic protection, the platform offered little visibility into modern threats and required continual investment in physical infrastructure.

"Our top priority was gaining visibility into the risks we faced," Rebelo said. "We had many integrations, APIs, and portals, but couldn't clearly see the risks those introduced."

The security team evaluated several vendors, including AWS and Imperva. After extensive proof-of-concept testing, Akamai **App & API Protector** stood out for both its capabilities and the support provided by local partner CPD.

"Akamai proved to be the best option for us," she continued. "During the proof of concept, we gained visibility we never had before."

As a comprehensive, all-in-one web application and API protection solution, App & API Protector helped the team make a surprising discovery. Applications it believed were well protected were at great risk. "Before, my team was in the dark. With Akamai, we finally understood the level of bot activity and malicious attempts targeting our applications," she explained.

The move also eliminated the constraints of hardware appliances. "With our physical WAF, we were limited by infrastructure," Rebelo added. "After moving to Akamai, we gained better visibility and no longer had those limitations. My team can now take quick action."

Stopping malicious bots without slowing the business

After gaining visibility into the volume of automated attacks targeting its applications, Cocamar took the next step by deploying Akamai **Bot Manager**. The solution detects and blocks malicious bots at the edge while allowing legitimate users and trusted bots to access applications without disruption.

"We now have a tool that identifies unauthorized access attempts, such as malicious bots trying to break into our network or applications," Rebelo said. "The solution enables us to automate traffic control and limit access."

Bot activity fluctuates throughout the year, particularly as the cooperative's digital services and seasonal operations change. Rather than constantly adjusting defenses, the security team can rely on Bot Manager to automatically scale with demand.

"The number of bots we see varies from month to month," she explained. "One month, Bot Manager might block 100,000 bots, and another month it might block 200,000. Knowing we have a solution that can manage any volume gives us confidence that our environment is secure while legitimate users continue to access our applications."



Akamai became an essential partner in raising our information security maturity.

Paula Rebelo
Executive Manager of IT, Cocamar Agroindustrial Cooperative

Containing threats through microsegmentation

While App & API Protector and Bot Manager strengthened Cocamar's internet-facing defenses, the security team also wanted to better protect its most critical internal systems. That led the cooperative to deploy **Akamai Guardicore Segmentation** to control access between servers and limit how far an attacker could move inside the environment.

"Our goal was to prevent unauthorized access to our servers," Rebelo explained. "Microsegmentation helps us determine who should have access to what, and only when they need it. There isn't one administrator with access to everything."

The highest priority was protecting Cocamar's in-house ERP (enterprise resource planning) system and the Oracle Solaris operating system that supports it. Together, they manage the cooperative's finance, human resources, manufacturing, and day-to-day operations.

"That environment is the heart of our operations," Rebelo said. "Protecting it from unauthorized access was one of our biggest concerns."

During the proof of concept, Akamai Guardicore Segmentation revealed communication paths the team didn't know existed. Servers that should have been isolated were exchanging traffic, exposing unnecessary risk. "The proof of concept showed us we were blind to certain communications between servers," Rebelo said.

The visibility provided by Akamai Guardicore Segmentation allowed the team to tighten policies, reduce unnecessary communication between systems, and better protect against lateral movement if an attacker gained access.

"Before, we couldn't clearly see how our servers communicated in the background. Now we can identify unnecessary connections and quickly segment the environment to reduce risk," she continued.

The deployment also strengthened Cocamar's broader security program by integrating with its vulnerability management tools. When vulnerability scans identify high-risk systems, Akamai Guardicore Segmentation can immediately restrict communication between affected servers, helping reduce exposure while remediation is underway.

As confidence in the platform grew, Cocamar expanded deployment from protecting 15 servers to securing more than 200. It moved the solution's Essential Policies into block mode, used ringfencing to isolate critical assets, and implemented service-level microsegmentation wherever possible.

The team also uses the solution to demonstrate cyber risk reduction to its cross-functional information security committee. "We present risks and simulated scenarios to the committee," Rebelo said. "In certain scenarios, we've demonstrated that using Akamai Guardicore Segmentation reduced the risk of **ransomware** payload by 93%."

Building a stronger security culture

Each Akamai deployment uncovered risks Cocamar didn't know existed. App & API Protector revealed hidden application risks and bot activity. Bot Manager quantified and controlled malicious automation. Akamai Guardicore Segmentation exposed unexpected server communications, excessive access, and opportunities to reduce lateral movement.

Together, these insights helped Cocamar move from reacting to threats to proactively managing cyber risk. The cooperative gained greater visibility and faster response capabilities. Those improvements enabled a more mature security program that continues to protect its most critical operations. "Akamai made our environment more secure, more manageable, and with less risk," said Rebelo.

For Rebelo, Akamai has become more than a technology provider. "Akamai is a great partner — not just in terms of tools, but throughout our journey of building a stronger security culture. Our information security maturity is at a whole new level, thanks to Akamai's tools," Rebelo concluded.

cocamar

Founded in 1963 as Cooperativa de Cafeicultores de Maringá Ltda, Cocamar Agroindustrial Cooperative initially brought together a group of 46 founders, all coffee growers, to organize regional production and to receive and process the product. Today, it ranks among Brazil's largest cooperative organizations and owns the largest and most diversified industrial complex within the Brazilian cooperative sector. Cocamar operates 100 facilities across municipalities in northern and northwestern Paraná, western São Paulo, and southwestern Mato Grosso do Sul, with a membership of approximately 14,000 producers involved in the cultivation of soybeans, corn, wheat, coffee, and oranges.

© 2026 Akamai Technologies | Support |
| Published 10/26