

Century Data Strengthened Customer Security

Cybersecurity provider strengthened customers' security postures with Akamai's integrated ecosystem



Increased business continuity



Exposed shadow APIs faster



Unified threat visibility

Securing modern business at scale

Century Data helps organizations strengthen **cyber resilience** by securing the APIs, applications, and infrastructure that power modern digital business. As AI use, SaaS tools, and partner integrations grew, customers lost visibility across their environments. They struggled to see where APIs existed, which ones were risky, and how attackers could use them.

With Akamai, Century Data expanded its ability to deliver API visibility, runtime protection, and integrated security across customer environments. This helped enterprises improve uptime, reduce unknown risk, and respond faster to threats.

Addressing growing API risks

According to Century Data's CEO Wellington Franham, customer concerns shifted dramatically as their environments became more interconnected. "Securing against AI threats became our customers' biggest demand," Franham explained.

APIs now connect apps, partners, cloud systems, and AI tools. In turn, companies have large attack surfaces that they cannot fully see. "The lack of knowledge about APIs is extensive," Franham said. "Many companies don't know how many APIs they have or which ones are exposed."

Century Data saw how attackers increasingly bypassed traditional perimeter defenses. "APIs are like shopping mall doors that are open and unmonitored or even unknown — so you don't know the risks," Franham recalled.

The company needed a way to help customers move beyond isolated API protection and toward continuous, end-to-end API resilience.



Location

São Paulo, Brazil
centurydata.com.br

Industry

Business Services

Solution

Security

Products

[API Security](#)

[App & API Protector](#)

[Akamai Guardicore](#)

[Segmentation](#)



Strengthening cyber resilience with Akamai's integrated security ecosystem

Century Data partnered with **Noname Security** before Akamai acquired it and evolved the solution into API Security. Even after this change, the consultancy was convinced that Akamai was the best partner. "What stood out was the maturity of Akamai's full platform," Franham explained. "That led us to deepen the partnership."

Century Data used integrated Akamai security capabilities:

- **API Security:** Finds APIs, detects risks, and protects against API abuse across the development lifecycle and runtime environments.
- **Akamai App & API Protector:** Secures web apps and APIs with WAF, bot defense, and DDoS protection.
- **Akamai Guardicore Segmentation:** Limits lateral movement and strengthens breach containment through AI-powered, software-defined microsegmentation.

Franham emphasized the benefit of integration. "Many security tools work in isolation," he said. "With Akamai, our customers can see from the edge into the internal network."

The integration enables customers to correlate API posture, runtime behavior, authentication anomalies, and network visibility. "You can see what is happening now and what happened before. This isn't possible with point solutions," Franham said.

Customers also gain a clearer view of both external and internal risk with an accurate view of their API inventory. "That helps teams respond much faster," he continued.

Helping enterprises uncover hidden API risks

Century Data works with organizations running complex environments. Akamai solutions have helped uncover duplicated APIs, shadow APIs, and insecure development practices.

"Akamai is one of the only vendors that integrates with the development side — the shift-left approach," Franham explained. "You can strengthen security as developers build APIs."

Century Data's customers can also better address unknown risks, which then translates to better uptime. In one case, a customer discovered more than 8,000 APIs inside their infrastructure.

Once suspicious behavior emerges, Century Data helps customers respond. "When a breach happens, we first identify which API or system is behaving unexpectedly and then block attacks," Franham explained.



Akamai gave us a full security ecosystem, from API visibility to internal segmentation.

Wellington Franham
CEO, Century Data

Strengthening network security with Akamai Guardicore Segmentation

While API Security protects customers' application layer, Akamai Guardicore Segmentation helps control what happens inside their networks.

Many organizations reach out to Century Data after a **ransomware** incident or audit finding. The same issues appear repeatedly: flat networks, limited visibility into east-west traffic, and internal controls that cannot keep up with fast-moving workloads across cloud and on-prem systems.

Before Akamai Guardicore Segmentation, these companies often managed segmentation through VLANs, internal firewalls, and access control lists tracked in spreadsheets. This created broad security zones, but no real visibility inside them. Any change often required a full network project, so segmentation work was delayed for years.

Akamai Guardicore Segmentation changes that approach. "Customers get a process-level map of east-west traffic," said Franham. "That visibility unlocks everything else."

Faster containment and real-world impact

Akamai Guardicore Segmentation also helps teams respond faster when attacks happen. Prebuilt ransomware policies can block common attack paths between workloads. This quickly shuts down the most common lateral movement paths used by attackers.

"Once customers see the solution in action, they often take advantage of its AI labeling and AI-driven threat hunting," Franham explained. "It becomes a full visibility and response platform."

This is especially important in environments with legacy systems, which are common in Brazilian enterprises. Akamai Guardicore Segmentation supports older operating systems that other tools often miss. It also works without depending on the network team's roadmap or a specific hypervisor. With a single console across on-prem, cloud, containers, and legacy systems, teams no longer need to manage firewall rules, security groups, and cloud policies in parallel.

In one example, a large Brazilian financial services customer with around 1,000 workloads spread across various service providers came to Century Data after a ransomware incident and the Central Bank of Brazil's BACEN audit. The company's previous segmentation project had stalled for more than a year due to complex VLAN redesign efforts.

With Akamai Guardicore Segmentation, Century Data deployed in phases. First came discovery and AI-based labeling. Then ransomware policies blocked common attack traffic. Finally, teams ringfenced key systems like ERP and payment platforms.

Within weeks, the company's high-value applications were isolated. PCI scope was reduced, the BACEN audit issue was closed, and the SOC team began using insight for threat hunting across the full environment.

Delivering local expertise with global security innovation

For Century Data, the partnership delivers more than technology. Akamai's investment in Brazil also helps the company support enterprise customers. "Akamai offers support in Portuguese, local services, and the expertise needed for large corporations like banks and retailers," Franham said. That local support helps Century Data build customer trust while delivering mature, enterprise-ready security solutions.

Franham also emphasized Akamai's ability to stay ahead of emerging threats, particularly in AI security and API governance. "Often, when a problem occurs, Akamai has already developed a solution," he said.

As companies use more AI apps, APIs, and connected systems, Century Data sees visibility and resilience as increasingly important. "Our partnership with Akamai allows customers to better understand risks, improve business continuity, and strengthen resilience.

And we expect Akamai to continue helping us address pressing customer needs even as they evolve," Franham concluded.



Century Data strives to make the world a safer place to live and conduct business by carefully researching, innovating, and developing solutions and services — with commitment and responsibility — through consulting, training, innovative solutions, and specialized services. We are obsessed with our clients' success, passionate about innovation, and committed to operational excellence in order to build long-term relationships. We work tirelessly to earn and maintain our clients' trust, and we do not rest until they are completely satisfied.