AKAMAI CUSTOMER STORY

Casio Blocks Sophisticated Bots with Akamai

Akamai Bot Manager Premier and Akamai Content Protector blocked 40M monthly scrapes and enabled site stability

Protected servers from load spikes

Blocked 40 million resale bot hits

Cut costs with AI detection

Casio Computer Co., Ltd., is a comprehensive manufacturer of electronic products, such as timepieces (including the G-SHOCK brand); educational products, such as scientific calculators; and audio enterprises, such as keyboards. In recent years, the company has expanded into new domains by offering products, such as the AI pet robot Moflin.

Casio brand products are beloved around the world, with overseas sales accounting for more than 80% of revenue in its timepiece enterprises. Their direct ecommerce sales also perform very well, and Casio is planning for further expansion in the future. Against this backdrop, Casio views the threat of cyberattacks and other security risks as an immediate concern, and has made "strengthening information security" one of its priority policies for business management.

A flood of bots is threatening global ecommerce sites

Within Casio, it's the Service Development Department, a part of the Digital Innovations Headquarters, that is driving the digital initiatives toward transformation with this approach. This department is responsible for a wide range of areas, including the development and operation of external websites and the promotion of cloud and AI use. Within the Service Development Department, the Web Services Team is responsible for managing the networks and infrastructure of Casio's ecommerce sites. By ensuring the stability of Casio's global ecommerce sites, the team improves the customer shopping experience, thereby contributing to increased corporate value.

CASIO

Location

Japan
casio.com

Industry

Manufacturing

Solutions

Bot Manager Premier
Content Protector

Akamai

The ecommerce sites that Casio directly operates had been managed with the expectation of traffic surges, such as those that occur during the launch of limited-edition models. However, in recent years, widespread attempts to make automated purchases using bots and AI have begun to threaten the stability of their operations.

Keita Sasazawa of the Service Development Department, Digital Innovations Headquarters, recalls one such incident during the launch of a new product. "Our ecommerce sites are operated on a regional basis. When we were launching the sale — a new watch model in a particular area — the sudden high concentration in traffic rendered the entire site unstable. In the immediate aftermath of this incident, we suspected a distributed denial-of-service (DDoS) attack, but struggled to identify the actual cause. But before long, it soon became clear that shopping bots that were targeting the new product were responsible.

"The bot traffic continued even after the item had fully sold out, making the ecommerce site unusable for normal operations for several days. The impact eventually spread across our global ecommerce sites. Massively scaled bot traffic and attacks pose a serious threat to the core of business operations. Addressing the threat of bots and whether we could secure both our conversion rates and sales had become critical issues," said Sasazawa.

Osamu Yoshizawa from the Service Development Department recalls the state of Casio's ecommerce site infrastructure at the time, saying "Our countermeasures were mainly focused on customer traffic surges and DDoS attacks, and we didn't have any bot-specific measures in place. As a result, we relied solely on server upgrades and the rate control function of our web application firewall (WAF). Looking back, we can say we went into the launch of a popular product without sufficient preparation."

In response, Casio urgently investigated their available options, and introduced Akamai Bot Manager Premier. "By using Bot Manager Premier to visualize bot activity and block access, we were able to improve site stability. This also heightened awareness within the company of bot countermeasures, and increased expectations for Bot Manager Premier," Yoshizawa reflected.

Blocking sophisticated bot requests with Akamai Content Protector

However, while the countermeasures to malicious bot technology are being bolstered, bot technology has also continued to evolve. "We have seen an increase in requests slipping through our bot defenses and launching attacks. This trend was particularly evident with products sold in January 2025," explained Yoshizawa.

> "Our company has been adopting Akamai solutions in progressive stages to strengthen our security. Having already proven their reliability and performance through their content delivery network, web application firewall, and Bot Manager Premier offerings, we had a high level of trust in Akamai already, so it was a natural next step for us to then roll out Content Protector.
>
> — **Keita Sasazawa**
> General Manager, Service Development Department, Digital Innovations Headquarters, Casio Computer Co., Ltd.

Akamai

This led to Casio adopting Akamai Content Protector. Yoshizawa explained Casio's reasoning: "We wanted to reduce the loads the sites were facing, so we started by analyzing their causes. We found that the majority of requests were simply for displaying the product page. Bot Manager Premier specializes in scoring the likelihood of bot access to web pages that require user input or active actions, such as purchase flows involving login processes, so a new angle of attack was needed.

"In contrast, Content Protector is particularly effective against bots that repeatedly refresh simple product pages to check stock status, referred to as content scraping. After conducting a proof of concept and evaluating the blocking performance of Content Protector, we decided to adopt this product as well."

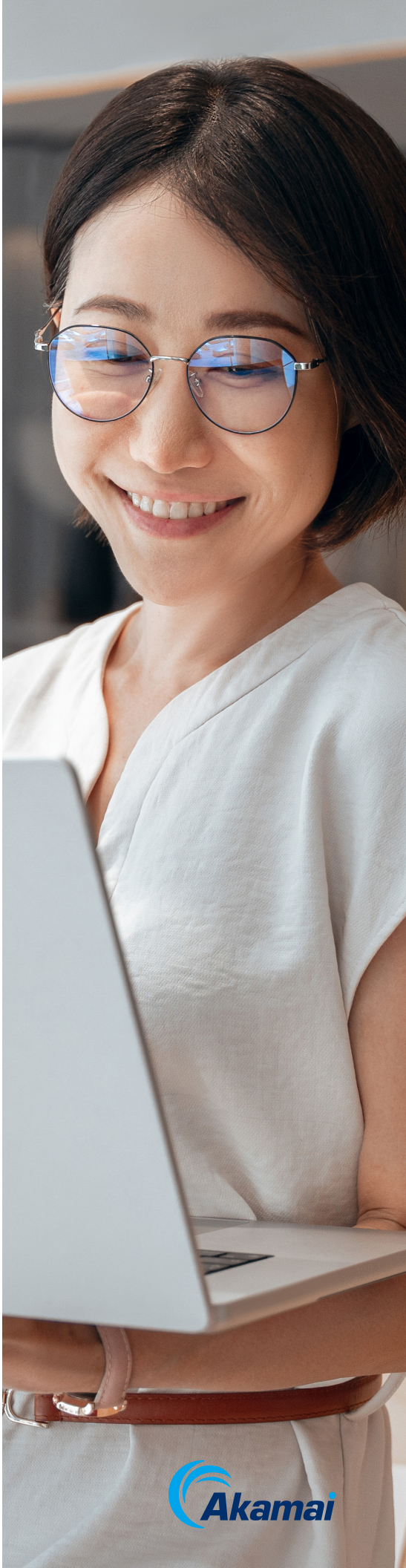
Ensuring continued ecommerce site operations

One of the benefits of introducing Content Protector has been the blocking of 30 million to 40 million unwanted scraping requests per month. "In the past, servers would sometimes go down during the launches of popular products, but now we are able to reliably complete sales processing. Even in the re-launches of popular products into other regions, we have been able to operate the ecommerce site stably and completely sell out of stock," said Sasazawa about the results of the actions they'd taken.

Furthermore, Casio has also confirmed additional benefits that they did not anticipate when they started. While Content Protector was originally introduced to counter both high concentrations of traffic during launches of popular products and scraping, it also had the benefit of proving effective against DDoS attacks. These days, it's become routine for large-scale DDoS attacks to be launched using bots. With its built-in capabilities for identifying malicious bots, however, Content Protector detects them with high precision.

In addition to limiting the volume of requests, it is increasingly important to examine the characteristics of each individual request and block them if they are suspicious. "With conventional rate limiting (limiting the number of requests per single unit of time), requests at a rate below a set threshold are considered to be legitimate, so bot requests sent at a slow pace could slip through the WAF rate limiting controls.

"However, Content Protector also has the ability to catch and detect these as well. In May 2025, we faced a DDoS attack involving about 60 million requests made in two minutes. In addition to blocking them with rate limiting, Content Protector detected and blocked about one million requests that slipped through the rate limiting controls," explained Yoshizawa.



Content Protector is also contributing to improvements in operations

Bots attack in various patterns, most often via scraping, but the addition of defense rules by Akamai's product team and automatic AI detection mean that Casio can keep on top of bots with techniques that evolve every day.

For Casio, product sites are the face of the company and, as such, are a vital point of contact with the customer that directly affects brand strength. Content Protector, which takes on the role of keeping business operations stable, is not just a security tool, but a strategic foundation that supports business growth.

High expectations for Akamai's protections against increasingly sophisticated AI-driven attacks

Turning to the topic of future developments, Sasazawa continued, "Cyberattacks are becoming increasingly sophisticated through the use of AI and other latest technologies. And the number of zero-day attacks, for which the countermeasures are unknown, are on the rise. We view them all as major threats to our company. To build defense capabilities that can withstand the latest technologies, we have great expectations that Akamai will provide solutions that can reliably protect us against even the newest types of attacks."

Yoshizawa expressed his appreciation by saying that "Maintaining the strength of the Casio brand through our ecommerce sites depends on the stable operation of our global platform, and in these current times it is especially important to have countermeasures against scraping by AI. We ask that Akamai continues to provide ways of dealing with these threats."

> "The costs, resources, and time required for tuning were reduced, along with our staff workloads. This has resulted in improved internal ratings for our overall security solutions.
>
> — **Osamu Yoshizawa**
> Leader, Development Group, Service Development Department, Digital Innovation Headquarters,
> Casio Computer Co., Ltd.

CASIO

Established in June 1957, Casio Computer Co. is expanding its ventures in timepieces, education (general calculators, scientific calculators, information communication technology [ICT], learning applications, electronic dictionaries), and electronic musical instruments, and is also getting involved in other new sectors, working with AI pet robots, embedded projectors, and medical equipment.

| Published 12/25

Akamai