DataDome

Harman defeats DDoS attacks, protecting revenue & customer experience with DataDome

DataDome.co

Harman defeats DDoS attacks, protecting revenue & customer experience with DataDome

Harman, a Samsung Company, is a global leader in connected products for automakers, consumers, and companies. They were faced with escalating DDoS attacks and bot threats targeting their e-commerce websites. Harman turned to DataDome to stop the bots, leveraging our rapid implementation and bot protection to maintain site reliability, especially during peak holiday seasons. With DataDome, Harman reduced revenue loss, minimized customer impact, and ensured seamless online operations, reinforcing its commitment to superior customer experience.

- ✓ **Millions saved in revenue**
- ✓ **Website reliability & improved UX**
- ✓ **Responsive support for crisis**

> "
> The biggest benefit was zero issues during the holiday season—everything was smooth. We had logs showing 16 attacks during that period, but no one even noticed. The websites just worked, which is exactly what we wanted.
>
> Julian Charnas
> Director of Digital Commerce at Harman

The challenge: ensuring website uptime amidst rising DDoS attacks

The availability and responsiveness of a website are key to its success. Harman is well aware of this, which is why, when their websites began experiencing intermittent outages and severe slowdowns due to DDoS attacks, the company reacted immediately. Julian Charnas, Director of Digital Commerce at Harman, recalls: "When the sites went down, all the alarms triggered. We saw a huge traffic spike, which wasn't due to a sales promotion; it was 10x or even 100x our normal traffic. It became clear that it was malicious traffic rather than organic."

These DDoS attacks brought some of Harman's e-commerce sites to a halt for periods of 10 or 15 minutes, which obviously had negative consequences in terms of customer experience and sales. But the real fear of the e-commerce team was that the attacks would continue or happen during peak sales.

"We were worried this was a prelude to a larger-scale attack, especially with the holiday season approaching. Our main concern was the risk of being down for hours during that period, which could mean millions of dollars in lost revenue," says Julian.

The risk wasn't limited to sales, as some of Harman's websites were also used as essential self-service support tools. Their inaccessibility was leading to higher customer service contact rates, which had associated costs. Harman needed a solution that would provide immediate protection against DDoS attacks and all bot-related threats.

The solution: bot defense, anti-DDoS, and fast integration

First, Harman tried several in-house methods to manage the bot attacks. Julian and his team implemented CAPTCHAs on submission forms and used fraud detection tools for payment tests to mitigate some bot activities. However, these measures were not comprehensive and did not prevent DDoS attacks, which were overwhelming their e-commerce infrastructure. **While security measures such as web application firewalls (WAFs) were in place for other internal applications, public e-commerce sites require a different approach as they must remain openly accessible to customers.** This left them exposed to various types of bot attacks.

"We considered managing the threats internally through some AWS services," admits Julian, "but as we were under attack, we needed to fix things quickly." Harman explored two solutions for bot management and online fraud protection: DataDome and a competitor. Ultimately, **they prioritized finding an external provider that could be implemented quickly, was cost-effective, and came with a strong reputation in the industry.** Julian was impressed: "The technical side was so straightforward that we were live within a week. Instructions were very clear, and the integration seamless."

DataDome's team provided comprehensive support during onboarding, helping Harman fine-tune their protections and optimize their defenses against current and future threats.

The results: zero incidents during peak sales season and millions in revenue saved

Harman saw around 16% of their site traffic identified and blocked by DataDome as malicious bots—a much higher percentage than they had initially imagined. During the critical holiday season, **DataDome proved invaluable, as Harman faced 16 major bot-driven attacks, which were effectively blocked** without a single incident of downtime or performance degradation.

Michael Gillman, Harman's Director of Digital Customer Experience, appreciated the smooth operation: "DataDome saved us from potentially losing a lot of revenue. The price was also competitive, and the implementation very quick."

The two e-commerce experts also enjoyed working with the DataDome Threat Research team, particularly during a recent card cracking activity. "Our payment fraud team alerted us that a large number of failed authorizations were occurring at our bank," relates Julian. "DataDome's Threat Research team quickly identified it as a sophisticated attack, using hundreds of IP addresses and browser signatures. They put a rule in place to block it within a day."

Would Harman recommend DataDome? "Absolutely!" shared their team.