

A government research laboratory uses Cloudflare's security solutions to detect and block 40% of unwanted traffic at the edge

Challenge: Unseen threats overloading infrastructure

Government research labs often handle large volumes of web traffic — but not all of it comes from legitimate users.¹ One lab had provisioned its infrastructure based on expected demand. But after deploying Cloudflare's security solutions, it uncovered a different picture: a significant share of the traffic wasn't from real users at all. Malicious bots and automated attacks were quietly consuming resources and driving up costs.

Solution: Cloudflare's DNS, DDoS protection, and bot management expose hidden inefficiencies

After moving its website behind Cloudflare's DNS and DDoS protection, the lab saw an immediate 20% drop in traffic — harmful requests were being blocked at the edge. But the biggest insight came with the rollout of Cloudflare's bot management tools: another 20% of traffic disappeared.

In total, traffic dropped by 40%. More importantly, the lab realized its infrastructure had been provisioned based on incomplete data. What appeared to be normal traffic was actually a steady stream of non-human and malicious requests.

Impact: Smarter resource allocation and cost savings

With Cloudflare blocking this unwanted traffic at the edge, the lab no longer needed to scale its infrastructure to meet artificial demand. They avoided costly upgrades, optimized bandwidth usage, and ensured their resources served real users — not malicious bots.

This case shows how Cloudflare's security solutions don't just defend against threats. They provide visibility into traffic patterns, uncover hidden inefficiencies, and help government agencies make smarter, more cost-effective decisions — all while securing their mission.

[Learn more](#) about how Cloudflare can help your agency protect, connect, and accelerate your mission.

Key Takeaways

- 40% reduction in unwanted traffic due to Cloudflare's DNS and DDoS protection in addition to bot management tools
- Hidden infrastructure inefficiencies revealed by increased visibility into traffic patterns
- Cost savings and optimized resource allocation due to better blocking of unnecessary and malicious traffic

Related Products

- [Bot Management](#)
- [DDoS Mitigation](#)
- [Cloudflare DNS](#)

"We unknowingly sized our services to include malicious traffic, and we're saying, look, now you have extra capacity just by turning on Cloudflare. You can almost double your capacity by blocking better." - CISO at a Government Laboratory