CLOUDFLARE

CASE STUDY

GovTech Procurement

GovTech Procurement secures Indonesian National Procurement Platform against bot and DDoS attacks using Cloudflare

GovTech Procurement, a division under Telkom Indonesia, was established by Presidential Decree No. 17 of 2023 to foster a national procurement ecosystem that is transparent, efficient, and accessible. Collaborating with Indonesian National Public Procurement Agency (LKPP) as a strategic partner, GovTech Procurement built the LKPP online procurement platform by integrating the planning, payment, documentation, and monitoring processes to improve transparency and enhance Indonesia's national budget efficiency.

As a government service, our aim is to deliver seamless and comprehensive procurement transactions that promote local products, support SMBs, and enable transparent transactions using the latest technology.

Challenge: Ensuring performance, security, and privacy in a national digital commerce platform

"We are accountable for the confidentiality, integrity, and availability of sensitive government and public data," explains Andreas Cendranata, Infrastructure & Security Lead at GovTech Procurement. "As Indonesia embraces digital transformation and digital platforms in an evolving threat landscape, creating a robust IT infrastructure with advanced security is increasingly important."

As it searched for the right partnership to help facilitate the secure, frictionless acquisition of goods and services across the country, GovTech Procurement's core cybersecurity priorities included:

Threat response: protecting against DDoS attacks, malware, and unauthorized access

System reliability, uptime, and performance optimization: providing a secure, scalable, and fast-performing infrastructure while minimizing unscheduled downtime

Data protection and privacy: ensuring data integrity and confidentiality while complying with international data protection regulations

"Maintaining the public trust is essential — any breach or downtime could significantly impact the reputation and credibility of our platform," says Cendranata. "We need to balance maintaining operational continuity, connecting to other government systems and third-party providers, and modernizing our legacy systems to support continuous, uninterrupted transactions."

GovTech Procurement by leap

Key Takeaways

- Mitigated persistent DDoS, bot, and data scraping attacks, improving availability and reducing unwanted origin server loads.
- Centralized encryption and site security for over 600 tenant websites, streamlining certificate management and improving performance.
- Offloaded static content to the global network, improving website load times while reducing server traffic and costs

Related Products

- Rate Limiting
- SSL for SaaS
- Web Application Firewall (WAF)

Cloudflare application security secures public services against persistent online attacks

“With government websites recognized by the National Cyber and Crypto Agency as the primary target of cyber attacks in Indonesia, as the government’s main provider of digital commerce services we needed to provide top-tier protection that could mitigate the risk of unauthorized access, data breaches, and the consequences of cyber threats like ransomware and DDoS attacks,” says Cendranata. “ Cloudflare provided the broad range of services we were looking for.”

Reaching out to Cloudflare, the agency first addressed the frequent attacks that threatened the platform. It began by implementing the Cloudflare web application firewall (WAF), the mainstay of Cloudflare's suite of application services, to secure its public-facing applications. Encouraged by the WAF's success in mitigating cyber attacks and by Cloudflare’s ease of implementation, the GovTech team rapidly expanded its Cloudflare use cases.

“Today we use most of the Cloudflare application security products. We used to get hit frequently with DDoS and bot attacks, but having Cloudflare shield our web properties has been a game-changer for us,” says Cendranata. “It effortlessly handles most attacks right out of the box.”

Using managed rulesets from the Cloudflare WAF alongside advanced rate limiting to block bots, DDoS attacks, and protect applications and APIs against abuse by throttling traffic that exceeds defined limits, GovTech Procurement neutralized the data scrapers that burdened its origin servers.

“Cloudflare has really stepped up our security, reliability, and performance game. By preventing attackers from making an excessive number of API calls, spawning multiple app incidences, and creating redundant database processes, we have sidestepped several attacks that could have affected both user confidence and our bottom line,” says Cendranata.

Next-level protection against sophisticated threats

Complementing its Cloudflare application services implementation, Cloudflare adds yet another layer of protection to GovTech Procurement’s applications and internal networks. To stop attackers from spoofing genuine IP addresses to gain access to internal networks, Cloudflare provides GovTech Procurement with secure, dedicated egress IP addresses.

“Cloudflare secures us against more advanced DDoS incidents — only trusted traffic from dedicated Cloudflare IPs can access our back end,” says Cendranta. “That has protected us from multiple sophisticated attacks coming from what appeared to be legitimate sources.”

Designed to facilitate regulatory compliance and promote international privacy and data protection standards, Cloudflare solutions also assist GovTech Procurement’s ongoing effort to provide its users and vendors with world-class cybersecurity, data handling, and IT governance processes.

Optimizing performance and reducing costs on the Cloudflare global network

Offloading the lion’s share of its static content to the Cloudflare CDN and implementing Argo Smart Routing to efficiently route platform traffic along the fastest available network pathway have also contributed to performance gains and cost savings across the platform.

"All our websites run much faster," says Cendranata. "Cloudflare reduces traffic to our origin servers, accelerates asset loading times, ensures faster service delivery, and protects our digital infrastructure."

SSL for SaaS — everywhere security at scale

In addition to its top-level .gov web properties, GovTech Procurement is also responsible for the security of over 600 regional websites, many of which still rely on legacy technologies. The platform secures these vulnerable properties using SSL for SaaS, the Cloudflare solution for SSL certificate management at scale.

Operating under the Cloudflare "everywhere security" ethos and configured using a single API call, SSL for SaaS provides centralized, easy-to-administer encryption, security, and performance services for every site in GovTech Procumnent's web portfolio. Providing both security and flexibility, SSL for SaaS protects each site via the main Cloudflare dashboard while enabling site admins to independently maintain content.

> **All our websites run much faster. Cloudflare reduces traffic to our origin servers, accelerates asset load times, ensures faster service delivery, and protects our digital infrastructure."**
>
> **Andreas Cendranata**
> Infrastructure & Security Lead, GovTech Procurement

"Cloudflare allows us to provide our tenant websites with the same high-level services that secure our primary domains. That includes accelerating performance and providing uniform security protection across all our domains," says Cendranata. "Managing certificates for everyone is remarkably efficient — Cloudflare streamlines and simplifies what used to be a complex, time-consuming process."

Since onboarding with Cloudflare, the infrastructure and security team at GovTech Procurement has been as impressed with Cloudflare's support as it is with the efficacy of Cloudflare products. Asked to elaborate, Cendranata highlights the Cloudflare support team's rapid responsiveness.

"Working with Cloudflare has been a great experience," he says. "During the implementation, everything went seamlessly and since then Cloudflare has responded immediately to every request or incident report."