DataDome | CAPTCHA SOLUTION BRIEF

The most user-friendly, 100% secure CAPTCHA

The challenge: Traditional CAPTCHAs frustrate users & bots easily bypass them

For years, traditional CAPTCHAs have been the front line of defense against malicious bots, striving to protect websites and mobile applications. However, as the digital landscape evolves, their limitations have become increasingly apparent.

The Solution: DataDome CAPTCHA

In order to safeguard both user experience (UX) and security, DataDome has engineered its very own secure and privacy-compliant CAPTCHA, protecting hundreds of websites and applications across various industries: from e-commerce and transportation to gambling and classifieds. DataDome's CAPTCHA is distinguished from any traditional CAPTCHA through advanced machine learning and our comprehensive detection data models that only deploy CAPTCHAs to traffic identified as automated bots, preserving the smooth experience for genuine users.

On the extremely rare occasion a human is challenged (which is less than 1 in 10,000), the DataDome CAPTCHA can be solved in under two seconds. DataDome monitors all requests in the background, and the CAPTCHA is only shown if our detection engine suspects the request is coming from a bot.

Drawbacks of traditional CAPTCHAs

- ✘ **No strategic CAPTCHA deployment**
- ✘ **Catch-all experience for both human and automated traffic**
- ✘ **Poor challenge design causes user frustration**
- ✘ **High rates of abandoned transactions and lost revenue**

Device Check: The first truly invisible challenge

- ✔ No setup required
- ✔ Full end user privacy preserved
- ✔ Zero interaction with end users
- ✔ Minimizes the use of visible challenges
- ✔ Supports web apps & SDKs

To provide an alternative detection layer and further preserve the seamless user experience without compromising security, DataDome offers an invisible challenge called **Device Check**. This challenge functions much like a CAPTCHA—but without any visible or interactive challenge to the end user. The authentication process occurs within the user's device, confirming device-specific signals via proof of work, all without any visible prompts for the end user.

Device Check works in tandem with DataDome CAPTCHA to validate human users and block malicious bots. In the event of bot-originated requests, Device Check promptly springs into action, either blocking access entirely or imposing a visible CAPTCHA challenge to thwart potential threats.

> "The use of CAPTCHA is complex and nuanced, offering both benefits and drawbacks. As such, some vendors are introducing invisible proof-of-work challenges to complement CAPTCHA."
>
> **- Gartner®**

Accurate & effective bot detection

DataDome CAPTCHA sets a new standard for identifying advanced and elusive bots right from their initial requests, especially when combined with Device Check. Unlike traditional security measures that often catch bots only after repeated suspicious behavior, our advanced algorithms are finely tuned to identify automation and malicious intent early on.

By seamlessly blending robust security measures with a user-friendly experience, our solution marks a significant step forward in safeguarding digital ecosystems. Trust in DataDome's commitment to innovation and protection, and unlock the possibilities that our integrated CAPTCHA offers for your online platforms. Secure your digital presence with DataDome CAPTCHA & Device Check—a smarter, user-centric approach to online security.

Key benefits of Device Check

- **Significantly reduces false positive rates**
- **Fewer unnecessary challenges for real users**
- **Reduces reliance on CAPTCHAs**
- **Smoother, more user-friendly online experience**

Frictionless user experience

Ensure your real users are very rarely challenged (if ever). Your platform responds instantly when DataDome detects a risk, increasing user trust and satisfaction with a seamless user experience.

User privacy

The verification process of our CAPTCHA is designed to collect and store *no personal information* during the assessment. Users can confidently engage with websites and applications, knowing that their privacy remains intact.