CSP frame-ancestors is the most important protection mechanism against external framing, and better than X-Frame-Options in multiple ways:

1. **CSP Frame Ancestors can run in Report-Only Mode**. This is a big deal when you want to roll-out protections on production systems in a safe way without causing regressions.
2. **CSP Frame Ancestors will send violation reports to your Report-Uri / Report-To**. This is super important for mapping out risks and observing your traffic (in monitoring or enforced mode).
3. **Unlike XFO, CSP Frame Ancestors** **covers Ancestors**. This means that it's more powerful and effective blocking for some use-cases like this report of a [wormable clickjacking attack](https://hackerone.com/reports/85624" \t "_blank).
4. **CSP frame-ancestors is more flexible**, allowing custom domains:  
   Content-Security-Policy: frame-ancestors 'self' mysubdomain.mysite.com https://frame.partner-site.com;  
   While this flexibility is theoretically supported by XFO ALLOW-FROM - in practice it is not supported

--> Use **BOTH** CSP frame-ancestors and X-Frame-Options for best protection and coverage across browsers.