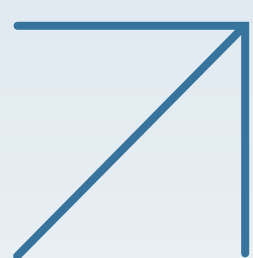


# 7 Must-Have Capabilities for Client-side Protection



Client-side attacks are on the rise in both size and frequency. Here are seven key characteristics to look for when evaluating your next client-side protection solution.



## 1. Access Your Advantage

Ensure robust client-side protection by seeking out a solution that offers complete control of JavaScript access to client-side data and code. This must-have feature prevents malicious scripts from swiping sensitive details like logins, cached application data and other client-side treasures.



## 2. DOMinate Cybercriminals

When attackers insert malicious JavaScript payloads onto your web page through its DOM (Document Object Model) environment, you've got a big problem. Keep cybercriminals away from your accounts with a client-side protection solution that prevents DOM-based XSS (cross-site scripting) vulnerabilities.



## 3. Fix That Leak

Bad things happen when your data gets leaked to unauthorized people. Malicious actors can use your personally identifiable information (PII) to initiate identity theft, breaches, credential stuffing, ransomware and more. Your client-side protection needs to be able to block unknown destinations and known destinations with illegitimate parameters.



## 4. Stop Party Crashers

Third-party origin control protects the software supply chain by only allowing the right third-party code to access the network. Without it, the supply chain could be left vulnerable to unknown or uncontrolled third-party code with the wrong level of access to data. You need client-side protection that automatically uncovers third-party services and provides detailed activity tracking.



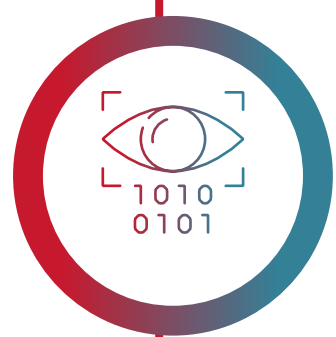
## 5. Catch the Drift

When you fail to detect changes at the asset and code level of client-side JavaScript, it's called JavaScript Drift. If you can't determine if code from third-party tools is potentially malicious, bad things can happen. Find a client-side protection solution that can identify code-level JavaScript changes on the client side, track the script activity and hash changes, and reevaluate the script risk accordingly. That way you'll be fully aware when danger arrives.



## 6. Win Your Storage War

Keeping your sensitive data in client-side storage (e.g., browser cache, LocalStorage, JavaScript Variables) puts it at risk. Ensure your client-side protection solution is advanced enough to protect against data theft with tools that dictate data sharing and more. Client-side browser monitoring is important as well and helps ensure data and content are only exchanged or shared with pre-determined domains.



## 7. Shore Up Security

Don't give cybercriminals an easy path to your data. Attackers seek out weak security configurations and poor security controls. Unfortunately, not all browsers adhere to the same security standards with all the common standards-based security controls built into them, such as iframe sandboxes, subresource integrity, and others. Make sure the client-side protection solution you decide on can detect and prevent digital trackers and pixels across your web properties.

Learn more about Radware's solution for [client-side protection](#).