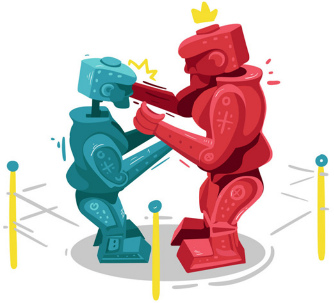
LOCKDOWN BROWSER VS. “LOCKED BROWSER EXTENSIONS”



A bare-knuckle cage fight

This isn’t really a bare-knuckle cage fight. It’s a straight comparison between LockDown Browser® and browser extensions that refer to themselves as a “locked browser.”

Let’s start with the similarities between LockDown Browser and the “locked browser” extensions:

- The browser runs full-screen and cannot be minimized
- Users cannot open a new tab or go to another website
- Certain keyboard functions, keystroke combinations, and mouse menus are disabled (e.g. printing, copy and paste, task switching)

This is where most locked browser extensions end. It’s better than nothing, but it’s like constructing a wall around 80% of the city – it looks formidable from certain vantage points, but the gaping hole leaves it open to attack.

LockDown Browser isn’t a browser extension. It’s a custom browser – a native application – for Windows, Mac, iOS and Chromebook. Why is that important? Because native applications have direct access to the operating system and the computing device (essential for stopping many types of exploits) whereas a browser extension is blocked from accessing key areas of the OS.

Here are some basic exploits possible with a “locked browser” extension but NOT with Respondus LockDown Browser:

- Virtual Machine, Sandbox and Safe Mode exploits
- Remote desktop and screenshare
- Extended desktop, multiple monitor, and screencast exploits
- Background applications used for communicating or question theft (IM, video recording)
- Applications launched with a timer, an incoming alert or message, or keystroke combination (e.g. Shift+@)
- Programmable and extended mouse buttons
- Browser cache and JavaScript injection exploits
- Task switching hacks and exploits

Not only is a native application like LockDown Browser better able to control the device and OS, it has the benefit of 20 years of heavy-duty use in the field. Thousands of educational institutions use LockDown Browser to protect hundreds of millions of exams annually. Through a partnership program, LockDown Browser is licensed by dozens of the largest publishers, testing centers, certification organizations, and assessment platforms throughout the world.

Implications for Automated Proctoring

Respondus pioneered “automated proctoring” more than a decade ago with the introduction of Respondus Monitor. Respondus Monitor is a companion application to LockDown Browser that uses webcam and computer vision to prevent and detect cheating during remote exams. Suspicious behaviors are automatically flagged for instructors, and each exam session is ranked in terms of overall risk.

A critical piece of automated proctoring is ensuring students don’t use the computer itself to cheat during the exam. Even if the computer screen is recorded, many exploits won’t appear in the screen recording video. For example, a video capture application started before the exam can run quietly in the background. Virtual machines, sandboxes and many other exploits won’t show in the video either. The bottom line: there’s no point analyzing videos of students smiling into their webcams, while they take advantage of exploits on the computer itself.

So, if you’re thinking of using automated proctoring for your students’ online exams (and we hope you are), be sure it includes the protection of LockDown Browser. Because a locked browser extension that safeguards only 80% of the online testing environment just doesn’t cut it.