Respondus Monitor: Risk Assessment of Hosted Architecture

Respondus Monitor is a companion application for Respondus LockDown Browser that enables students to take online exams in non-proctored environments. Students use their own computers with a standard webcam to record assessment sessions.

Why is Respondus Monitor only available as a hosted service?

There are several reasons we host Respondus Monitor on Amazon Web Services (AWS). First, it provides an immensely powerful security and control environment, including certifications for SOC 1 (SSAE 16/ISAE 3402), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FIPS 140-2, and more. We are confident the AWS environment can meet or exceed the compliance requirements of any university or school district. (For more details on AWS security, see http://aws.amazon.com/security/).

We also chose AWS for performance and scalability. The servers are continually monitored for health and performance metrics, with servers added or removed automatically to maintain a constant performance level regardless of load or individual server failures. Most universities don't have dozens of servers standing by, waiting for peak periods that may only occur a few (but critical) times a year. Using AWS infrastructure, we are able to handle these peak periods while avoiding the costs associated with idle capacity.

The third reason is cost. We achieve significant economies of scale by using AWS for all implementations of Respondus Monitor. If institutions had to maintain their own servers (up to 6 separate servers) the cost could greatly exceed the license for Respondus Monitor itself. In addition, our development and support costs are significantly reduced by supporting a single framework and architecture, which allows us to price our service competitively.

How Does Respondus Monitor safeguard student videos?

Security wasn't an after-thought for our architecture – it was our starting point. The best way to demonstrate this is to follow a video session through our architecture and see how data is secured every step of the way.

A student video session starts with LockDown Browser up-streaming the video using encryption that is unique for each session. The video is stored on servers that aren't accessible from the Internet. The server only accepts streaming connections, and only then from an internal server.

When an instructor wants to review the recorded videos, he or she must first authenticate with the learning system server to access the Respondus Monitor dashboard. All communications between the learning system server and the Respondus Monitor servers occur over HTTPS and the payload is encrypted using a unique key for each institution.

The Respondus Monitor servers render the video review UI but they don't have any access to the stored videos. An exploit on these servers, even at root, is not enough to gain access to the student videos. The video files can only be accessed when the request occurs from the Respondus Monitor servers using the unique key (supplied via the server plugin) for that institution.