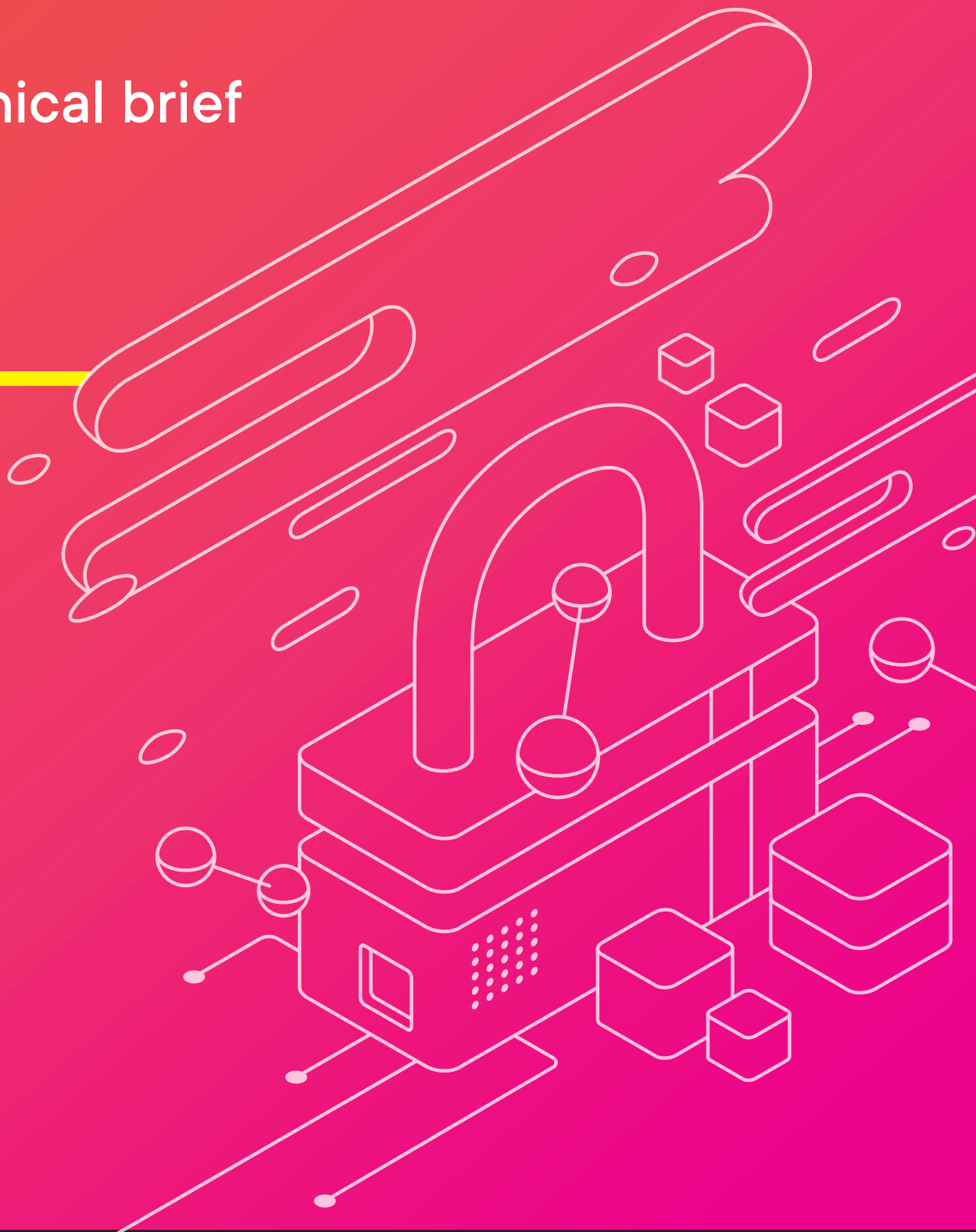
PLURALSIGHT

Deploying cloud labs within a secure environment

Technical brief

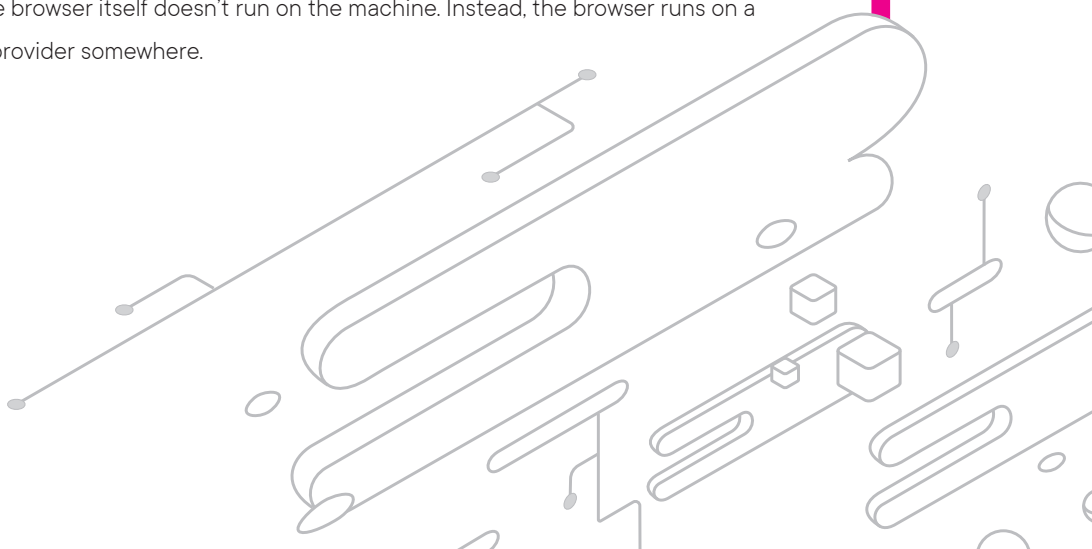


Cloud labs within Pluralsight Skills are curated environments that support step-by-step practice in public cloud infrastructures (e.g., Amazon Web Services, Microsoft Azure and the Google Cloud Platform). As such, some organizations prohibit the use of these public services due to security constraints. This paper discusses the various approaches you can take to leverage cloud labs while adhering to your security controls.

Deciding the right approach

When deciding how to deploy cloud labs at your organization, there are many factors to consider, including the end-user experience, your security level and how you'll achieve the right balance between the two. Organizations have been able to deploy cloud labs using one of the four approaches below:

- **Approve Pluralsight Skills' cloud lab experience through a security risk review.** Pluralsight products are built with security by design principles and we've implemented many of the controls organization's need to approve the use of cloud labs. This paper will not discuss the security practices in place. However, if this is a possible solution to explore, please reach out and ask for the following security guide: [Product] Cloud labs security white paper.
- **Allow access to cloud labs through your BYOD (bring your own device) policy.** Most organizations have allowed employees to unify their work and personal life under one device through a BYOD strategy. If this is the case for you, Pluralsight can integrate into this policy, enabling learners to access cloud labs safely from their devices.
- **Deploy virtual machines to allow access to cloud labs.** A smooth learner experience is crucial in enabling individuals to learn on company-issued devices. However, allowing access to public cloud labs requires adhering to a unique set of controls. You can deploy purpose-built virtual machines like Citrix or VDI to limit a user to specific tasks on the virtual machine (e.g., accessing cloud labs).
- **Use third-party tools that enable a secure browsing environment.** A web browser, the same application that connects users to the entire Internet, also connects users to internal applications. To keep those devices and the data they hold or access safe, enterprises have started to deploy browser isolation services where the browser itself doesn't run on the machine. Instead, the browser runs on a virtual machine in a cloud provider somewhere.



BYOD policy

Many organizations have a BYOD strategy in place with the goal of minimizing their risk. Generally, these devices will have the least amount of access to corporate data and can connect to public cloud services. Enabling learners to leverage their own devices is the easiest way to deploy labs across an organization. BYOD policies help in minimizing the surface area for data leakage.

Pros:

- Easy to set up by exposing the Pluralsight SSO URL to a user's BYOD policy

Cons:

- Learners must have a personal device when accessing cloud labs
- Organizations could see low adoption for labs due to the higher barrier to entry
- You need to educate learners on how to access cloud labs

Virtual machines

Organizations want to ensure that their end-user experience in the corporate system is as frictionless as possible. Although BYOD policies are easy for organizations to implement, it may miss the mark in terms of the end-user experience since it requires a user to have two devices. Alternatively, you can provide employees with unique build virtual machines (VMs) / Citrix that have restricted access to corporate data and connect to the public cloud.

Pros:

- Learners can access cloud labs through their work device

Cons:

- Limited numbers of VMs available to learners to access cloud labs (e.g., 1000 learners and five VMs)
- You must enforce specific access controls to ensure only the public cloud is exposed

Secure browsing environment

Browser isolation services are a new trend in which the browser itself doesn't run on the learner's machine. Instead, the browser runs on a virtual machine in a public or private cloud provider. This approach gives your learners the best experience; however, it requires additional investment in vendors who provide this technology. Some of the companies working on this trend are:

- Citrix Workspace (featuring Citrix Virtual Apps and Desktops)
- Menlo Security
- Symantec Web Security Service

Pros:

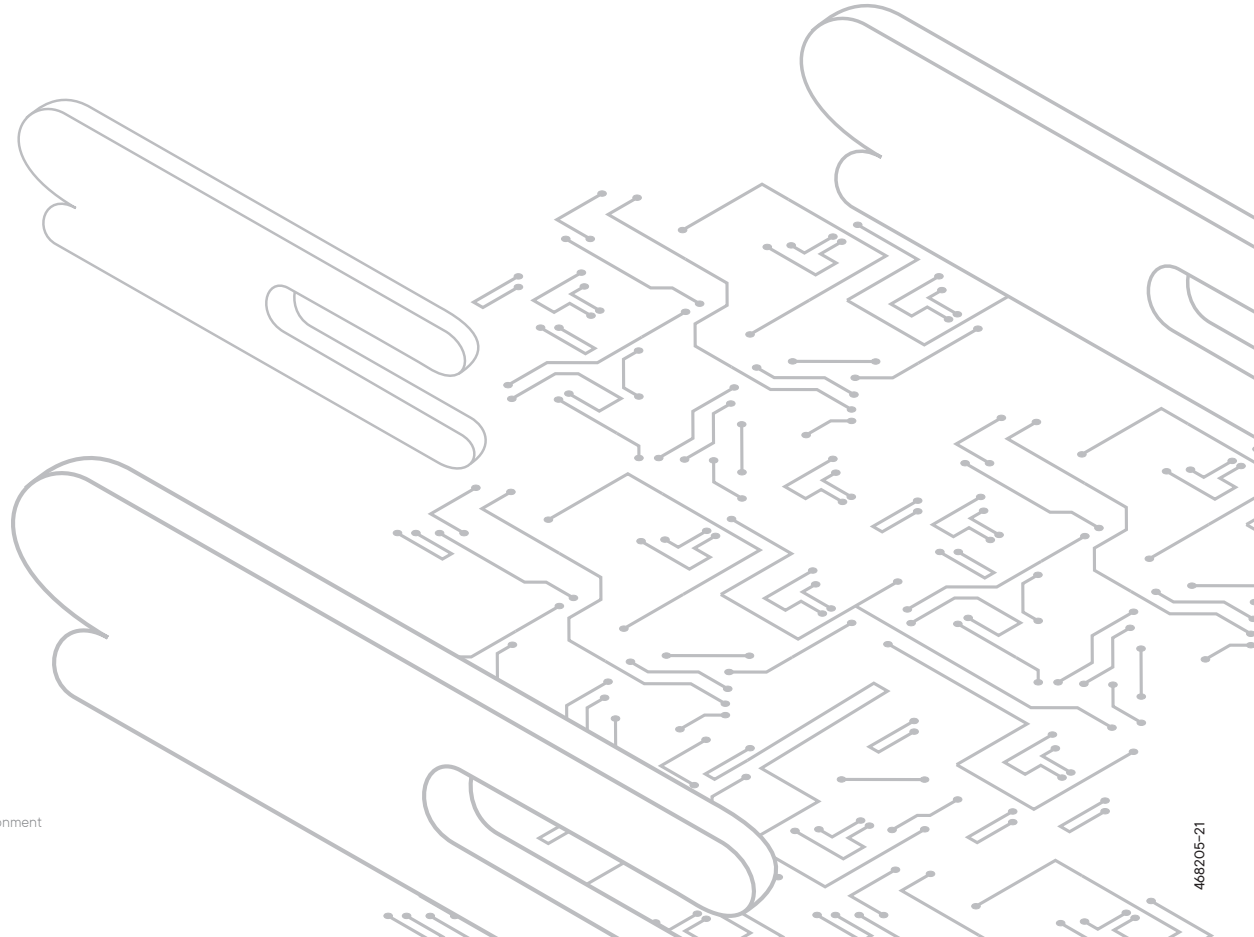
- Learners can access cloud labs within their workstation

Cons:

- You need to invest in specific vendor software to provide browser isolation to end-users

Conclusion

Pluralsight Skills' cloud labs experience allows learners to practice new skills in a safe, provisioned cloud environment. Even if your organization is in a highly regulated industry, there are various solutions available to help you mitigate risk and still empower your teams with valuable hands-on learning experiences.



468205-21