Pulse Secure®

Cloud Secure Access
IT Services: Step-by-Step Guide

In the next two years, combined IT infrastructure spending on private and public cloud will eclipse spending on traditional data centers, according to research firm IDC. Furthermore, a recent survey by LogicMonitor found that an estimated 83% of enterprise workloads will be in the cloud by 2020. Yet two-thirds of IT professionals say security remains their greatest concern in adopting an enterprise cloud computing strategy.

This step-by-step guide will help you navigate through the process of integrating secure access into your multi-cloud IT service model (ITSM) for each new business application or initiatives you are presented with.

1 Buy, build or migrate?

When faced with a new business initiative or application, the first decision point is determining whether you are migrating or porting to existing application infrastructure, starting with new data/infrastructure or buying an off-the-shelf SaaS solution with turnkey capabilities.

2 SaaS, data center, public or private cloud?

Once you've defined the buy/build/migrate approach, the next step is determining where in the multi-cloud will meet the requirements and be most cost-effective – in the data center, public or private cloud, or via a SaaS solution hosted by the application provider.

3 Outline secure access IT service scope and process.

As with any new initiative, you'll need to define the secure access project scope and priority along with the individual requirements.

4 Map groups, apps, resources, and security requisites.

Identify access scenarios by group, application and other factors. You'll need to clearly identify and document the component relationships as this, combined with the security requisites, are the basis of your multi-cloud secure access ITSM policy.

5 Build, refine and test your secure access policy.

Start with the visibility to refine and preempt any usability issues before they become issues. Remember to lead with visibility to fine tune and avoid having a negative impact on user experience wherever possible.

6 Notify users of your new policy, technical support protocols, SOC, and audit.

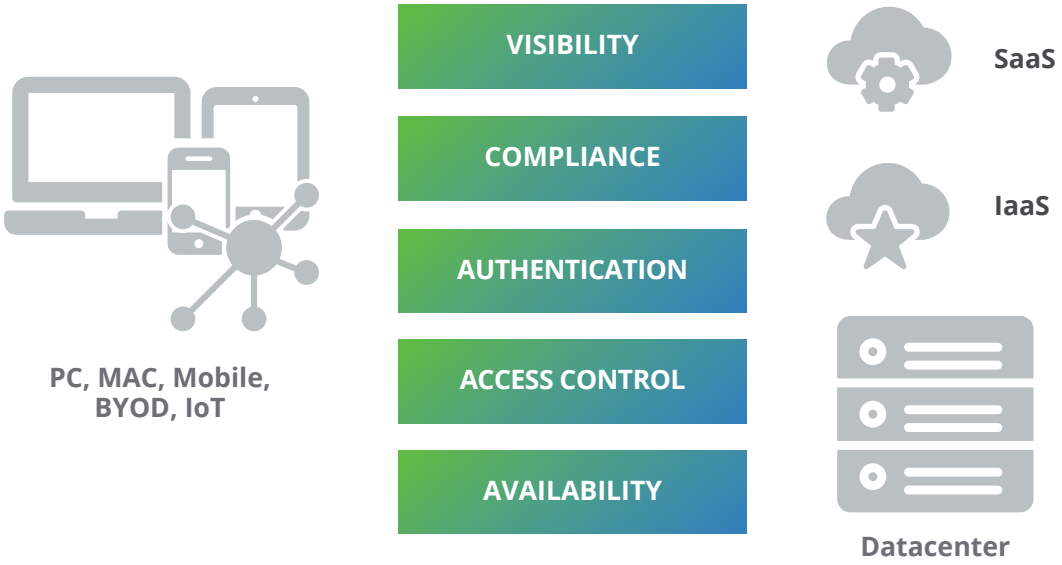
As you probably well know, users don't like abrupt change. Advance warning and plenty of clear, concise communication is key. Phase in your multi-cloud secure access policy rollout to change user behavior.

7 Verify. Tune. Examine areas to integrate, automate.

Document achievement and improvement and extend scope if necessary. To create a closed loop system, be sure to audit the process is working as planned – including user perceptions and potentially impacted productivity and workflow. Make any adjustments necessary to achieve optimal results and continue the audit cycle periodically to ensure effectiveness and relevance amidst changes in infrastructure and perceptions.

Solving access control used to be easy.

In today's Hybrid IT environment, it's not as easy as it used to be.



About Pulse Secure

Pulse Secure, LLC offers an easy, comprehensive Secure Access solutions that provide visibility and seamless, protected connectivity between users, devices, things and services. Our proven platform uniquely integrates cloud, mobile, application and network access to enable hybrid IT. More than 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net

Corporate Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net