




Which E-Signature Deployment Option is Right for You?

	 PUBLIC CLOUD	 PRIVATE CLOUD	 ON-PREMISES
CRITERIA			
Definition	<ul style="list-style-type: none"> An instance of the e-signature application runs on a server, serving multiple client organizations (multi-tenant), and is managed by a third party (i.e., the e-signature provider). 	<ul style="list-style-type: none"> An instance of the e-signature application runs on a server, serving a single client organization (single tenant), and is managed by a third-party (i.e., the e-signature provider or other service provider). 	<ul style="list-style-type: none"> Organization hosts their own instance of the e-signature application on their own servers behind their firewall.
Implementation	<ul style="list-style-type: none"> Fastest to implement Leverages a ready-made platform which has already been provisioned, implemented, and tested by the vendor. 	<ul style="list-style-type: none"> Get up and running quickly Leverages a ready-made platform which has already been provisioned, implemented, and tested by the vendor. You can select different deployment tenets to meet your business and technical requirements without the need to engage your IT resources. 	<ul style="list-style-type: none"> Longer to implement Takes time, personnel, and equipment to set up a new environment to meet your project requirements.
Support & Maintenance	<ul style="list-style-type: none"> Minimal IT dependency for application maintenance. Vendor is responsible for infrastructure risks to ensure high availability and disaster recovery. 		<ul style="list-style-type: none"> You are responsible for maintaining the application; your IT is responsible for ensuring high availability and disaster recovery.
Control			<ul style="list-style-type: none"> Full control over your infrastructure and apps to meet your corporate standards.
Upgrade Cycles	<ul style="list-style-type: none"> SaaS upgrade schedules are controlled and set by the vendor, who typically inform customers of product and system upgrades. IT involvement during upgrade is minimal. 	<ul style="list-style-type: none"> You have decision authority on timing and functionality of an upgrade when compared to public cloud. Your involvement is limited during a validation review. 	<ul style="list-style-type: none"> You own the responsibility for upgrades (more time and money involved).
Cost	<ul style="list-style-type: none"> Lowest upfront cost. Low internal resources required for support. 	<ul style="list-style-type: none"> Lower upfront cost vs. on-premises, but higher vs. public cloud. Low internal resources required for support. 	<ul style="list-style-type: none"> Highest upfront costs compared to cloud due to infrastructure and IT & support staff needs.
Security & Compliance	<ul style="list-style-type: none"> SaaS applications deployed in the cloud can be highly secure with expert supervision of network and server security. Look for the types of security and compliance programs that the vendor (and their infrastructure provider) has in place such as SOC 2 and FedRAMP. 		<ul style="list-style-type: none"> The responsibility is yours to ensure relevant security and compliance programs are in place.
Scalability	<ul style="list-style-type: none"> Solution can be easily scaled up or down (i.e., across multiple use cases and lines of business – locally and abroad) with little time and effort. 		<ul style="list-style-type: none"> Your IT team is responsible for planning system capacity requirements and work with business stakeholders to ensure scalability across current and new use cases per line of business.
Data Privacy	<ul style="list-style-type: none"> Vendor can help you meet data privacy and data residency needs by hosting the SaaS application in your country or region. 		<ul style="list-style-type: none"> Data privacy and residency rules are set by you.