Cloud vs On-Premise vs Hybrid

There are some industry standards and government regulations that require corporations or government agencies to implement an on-premise solution. While other industries and government agencies have the flexibility to choose to host everything in a cloud environment. An on-premise implementation is one where the servers reside within an organization's premises giving full visibility and control of the hardware, data and crypto keys to the data owners, where as a cloud implementation, a third-party hosts the hardware and often administers the set up and connectivity.

With most mobile security vendors abandoning support of on-premise installations, SyncDog is committed to the success of even our most demanding customers and therefore supports both cloud implementations, as well as on-premise implementations – plus we have worked with clients who require a combination of the two, or a Hybrid version.

- Cloud implementations are one of the easiest set-up and implementation options for organizations who want to deploy an end-to-end security solution quickly out of the box. Full organizations can be set up in a matter of minutes to hours using SyncDog.
- For those who want full control of their environment and full control of their crypto keys, SyncDog also supports on-premise deployments. This option allows organizations to deploy the same server-side relay, transport, and management tools as the cloud, in a local environment.
- Hybrid setups are less common, but SyncDog does support a wide array of custom deployments with the ability to have partial infrastructure in the cloud and partial internal.

Regardless of the option chosen, SyncDog's guided installers make setup simple, and our tools - like bulk user import - allow administrators to configure their environments with ease. Our intuitive grouping/sub-grouping methodology means customizing the setup to meet the needs of various roles or titles within the organization – down to the individual – is now an asset to be leveraged. With all other mobility solutions, this can add weeks to months to the implementation. Furthermore, SyncDog even supports redundancy and failover configurations for high availability to ensure mission critical data is always accessible. Finally, no matter the situation, we offer to work with our customers individually to support their custom or unique needs.

SyncDog provides a containerized solution that creates a vault for multiple applications and provides centralized management functionality for administrators. The solution offers a FIPS 140-2 Certified, AES 256-bit encrypted, end-to-end mobile security solution. The modular solution enables organizations to custom fit their mobility policies and security measures and align them to the specific needs of the various roles and titles of their entire employee base — down to the individual user. It will no longer matter if the device is iOS or Android, Managed or Un-Managed, Corporate/Government Owned or personal (BYOD) — all can be supported through a single solution. SyncDog protects and manages the device, detects, and prevents malware/phishing and other intrusions, encrypts, and isolates all the corporate or government data/files/apps that are accessed by or stored on the device and offers a private app store for distribution of internal native or hybrid apps. SyncDog can be hosted in the cloud (SaaS), on premise, or hybrid. All from a single vendor, from a single download and centrally managed in a single administrative console.

+1.855.SYNCDOG (1-855-796-2364)
info@syncdog.com

1801 Old Reston Ave, Suite 301
Reston, VA 20190