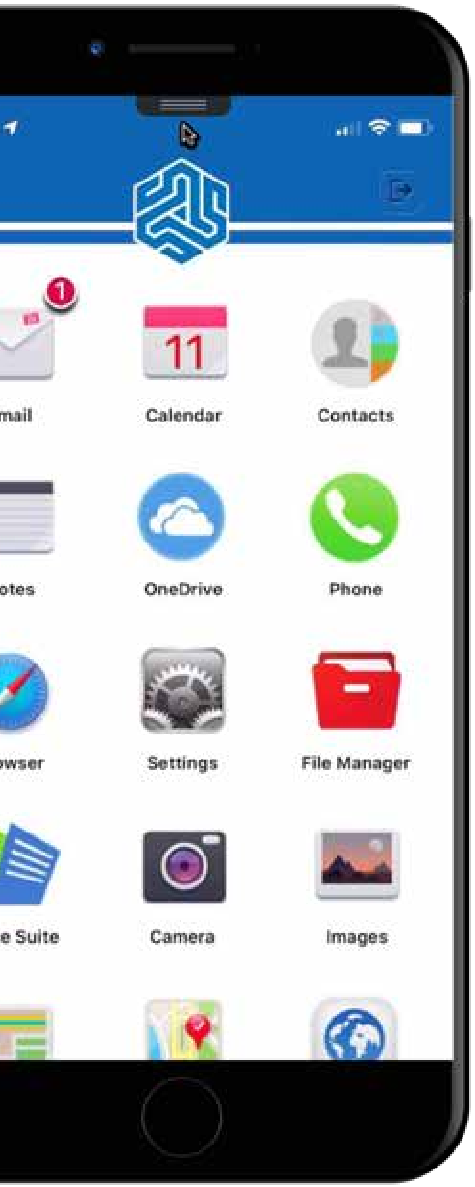
# SyncDog vs BlackBerry

Blackberry's initial promise of advanced mobile security by encrypting data in a device independent secure container has fallen far short of its goals. Government agencies, large corporations and numerous other organizations are rapidly abandoning their Blackberry environments based on difficulties and delays in set up, low user adoption due to non-intuitive user experiences, as well as difficulties in management and maintenance of the solution. This is because of most of the product acquisitions that were made over the years, have not been integrated into a single solution set. SyncDog is now the go-to solution for organizations in both the public and private sectors who rely on mobile device usage across its employee base yet need to ensure their internal and customer related data is always secure.



SyncDog allows government and businesses to implement a true device agnostic mobility solution that supports both "employer owned" as well as "personally owned" devices. SyncDog can flex to meet the needs of the various roles and responsibilities of the workforce by offering deep policy management of the device containers via an easy-to-use web-based console. The centralized management console allows administrators to have continuous visibility into their organization's mobile deployments, constantly keeping their finger on the pulse of user activity, device status, and operations. Policy management allows the organization to maintain control of their data by controlling the who/what/when and even where data usage is allowed, while still providing users with flexibility and access to the resources they need to be productive. For organizations needing to manage and inventory large number of devices, SyncDog also offers MDM functionality to enable device management and control.

> **Again, SyncDog is the only solution to finally deliver on the promise of full mobile device and data security in a single app, single download single sign-on solution that is device and operating system independent and works on both managed and un-managed devices.**

Furthermore, SyncDog offers access to more applications than just email, calendar, and contacts. To increase productivity for end-users; email, calendar, and contacts are essential functions used daily, but they aren't the only functions that are critical. Document management and sharing is another important function that must be secured. Additionally, web browsing, and messaging are other prime examples of commonly used functions in which security is a high priority. Unlike Blackberry, the SyncDog platform offers access to all these essential business functions, in a single, secure, and encrypted environment.

**Additionally, SyncDog does not require the use of a VPN to access the corporate/government data on a mobile device. There are many reasons why SyncDog was architected to not require VPN access:**

VPNs can be difficult to configure and manage and are prone to easily disconnect and interrupt work being done.

VPN's only secure the transport data, doing nothing to secure data at rest on the device.

Most importantly, VPNs create tunnels from outside the network, into the network, which means that packets are travelling from outside the network to internal network resources. This can be risky because permissions in VPN implementations must be managed carefully to ensure the user can only access limited resources externally in case the device is compromised with malware that attempts to silently access or discover other network resources. This is one of the biggest no-no's when establishing a **"zero-trust"** environment.

Zero Trust People
Zero Trust Location
Zero Trust Network
Zero Trust Assets

In contrast, SyncDog's solution queues encrypted packets outside the network DMZ which does not allow an infected device to discover or access other local resources through the firewall – aligning perfectly to cybersecurity best practices.

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.