The SyncDog SentinelSecure™ Mobile Workspace

Extending Military-Grade Security to your Mobile IP, Data and Applications

The SyncDog SentinelSecure™ containerized mobile workspace was built in response to market demand for an affordable best-of-breed solution with military-grade security and fast-deployment capability. SentinelSecure™ operates with the security and functionality to maintain workplace productivity across the outer reaches of your network perimeter.

SentinelSecure™ provides a great balance of end-user productivity and corporate data governance from a leading Independent Software Vendor (ISV) with more than 15 years of mobility development experience. SyncDog provides multiple purchasing scenarios for SentinelSecure™ and the container can be procured as stand-alone product or integrated component of an Enterprise Mobility Management (EMM) system from any of SyncDog's solution partners. For more information on SyncDog EMM partners, please visit www.syncdog.com/partners/.

The SentinelSecure™ Mobile Workspace Application Set

- **Secure Communications**
  - » Email Client: Securely access your enterprise ActiveSync, Exchange, Office 365, or Gmail accounts along with contacts in a self-contained workspace. Supports email attachments and links
  - » Calendar: Securely access your enterprise Exchange calendar. Full support of Month view, Week view, day view and agenda view
- **Secure File Management**
  - » Provides admin capability to securely post documents to a centralized filestore that synchronizes to the latest file versions, then pushes the documents to end-users. Also includes secure two-way synchronization of files across network filestore and remote device.
  - » Includes Office Suite, Secure Camera/Image Roll, Secure SharePoint access
- **Secure Internet/Intranet Access**
  - » Secure Browser: Browse the web without ever leaving the security of the container. Includes AES 256-bit encrypted back-office network connection for auditing/compliance.
  - » HTML 5 Hybrid Mobile App Frameworks: Securely run hybrid apps hosted in proprietary app frameworks. Hybrid apps remain within the secure confines of the container.
  - » Secure Chat and Messaging: Mobile chat client where data and communications are kept within the secure container using Extensible Messaging & Presence Protocol or XMPP.
- **Secure Location-based Services**
  - » Geo-Location and Tracking: Secure service capability that identifies device location then stores geo-location data so you can track the movement of the device over time. Includes storage and auditing capability.
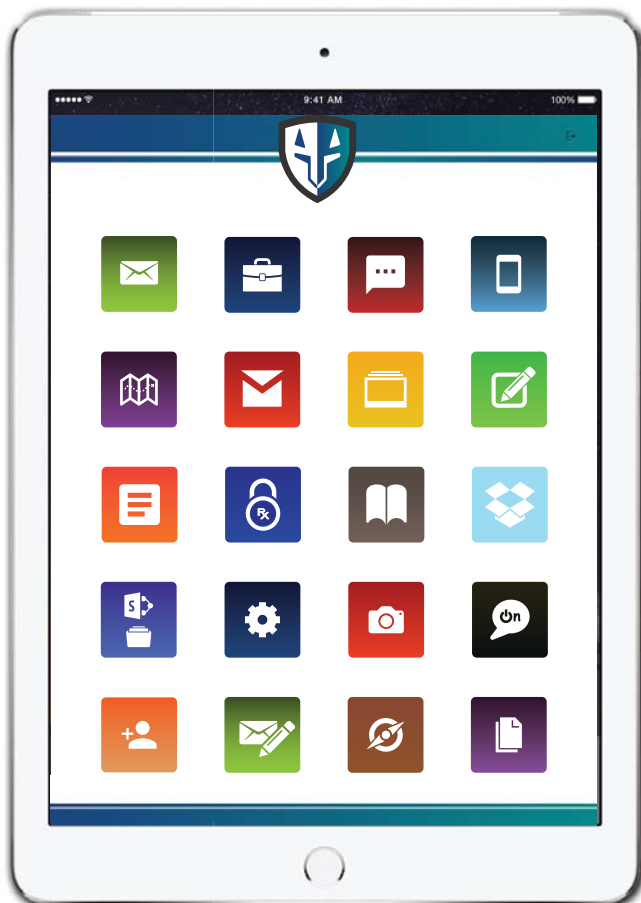
SYNCDOG

www.syncdog.com

SentinelSecure™ delivers military-grade secure mobile device partitions or "containers" that can secure emails/contacts, calendar items, IM apps, Internet browsers, mobile file stores and other business apps provisioned on personal devices to be used in a BYOD or COPE (corporate owned personally enabled) setting. The SyncDog architecture protects both data at rest and data in transit through Federal Information Processing Standard or FIPS 140-2, AES 256 bit encryption. SentinelSecure™ can be provisioned across the SyncDog Sentinel Server, a flexible agent-based MDM platform, or with any EMM/MDM solution.

SentinelSecure™ Delivers Application Workflows For:

- **Secure Communications**
- **Secure File Management**
- **Secure Internet/Intranet Access**
- **Secure Location-based Services**

MIGRATING FROM EXISTING CONTAINER SOLUTION IS EASY!

SyncDog is the leading ISV offering containerized mobility platform solutions and here are 4 reasons why you should consider an ISV-designed solution as you migrate:

1. Because SyncDog is smaller and works more collaboratively with partners and clients, we are able to keep step with market trends and be more responsive to evolving customer requirements.

2. Because of 1 above, SyncDog remains more focused on problem solving at the client level – we don't try to force what we think you need; we provide what you (the marketplace) has asked for. We know containerization well and are focused on building a roadmap that supports a best-in-class container.

3. ISVs like SyncDog offer more flexible payment options and solution builds that fit customer needs and development requirements. We are willing to work with customers on flexibly-priced solutions that fit a need (see our Dept. of Defense and Healthcare solution builds) with budget requirements considered.

4. ISVs like SyncDog build solutions that hone in on functional excellence. There is arguably no such thing as "out of the box" anymore because Enterprise IT is a heterogeneous collection of solution complexity with siloed human resources struggling to manage it. We understand that one size will never fit all and build ease of integration into our architecture.
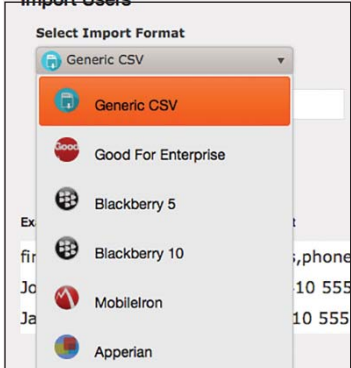
HOW EASY IS SENTINELSECURE™ TO MIGRATE?

For the most part, you or your systems admin just needs to:

1. Log in to the SentinelSecure™ dashboard, then

2. Go to the wizard in SentinelSecure™ and in a few clicks your users are automatically added.

If you're weighing the pros and cons of a lengthy, difficult migration to BlackBerry Enterprise Server, you owe it to yourself to see what SyncDog has to offer in solution functionality and ease of deployment, and customer experience. See for yourself how easy migrating to SentinelSecure™ can be.

Visit SyncDog.com/migration for more information.

SentinelSecure™ ships with multiple migration options built in.

SyncDog SentinelSecure™ Integration

SentinelSecure™ ships with integration to a multitude of Enterprise Mobility Management (EMM) systems. With SentinelSecure™, you get a military-grade containerized workspace that serves as a complementary layer of security to your existing InfoSec investment. Your mobile devices are fortified and your network perimeter remains secure.

SentinelSecure™ is currently integrated with the following EMM solutions: MobileIron, Notify Technology, Inc., and Snow Software. For more info on integration please visit syncdog.com.

SYNCDOG SENTINELSECURE™ & BYOD, COMPLEMENTING EXISTING INFRASTRUCTURE SECURITY POLICY

SentinelSecure™ reinforces enterprise security using an application workspace to protect proprietary enterprise data and IP (at rest/in transit) across a FIPS 140-2 certified solution. The containerized workspace delivers an added layer of security at the far reaches of your network perimeter, protecting you against:

- Malware: Seemingly safe games and consumer applications aren't always what they appear to be. With SentinelSecure™ your org's data and workspace apps on the device, along with the device's connection to your network, is physically separated from the rest of the device, keeping enterprise data and IP secure.

- Malicious Networks: If an employee unknowingly connects to a non-secure network that has data-harvesting capabilities, the device may be compromised but the corporate applications and data remain secure within the SentinelSecure™ workspace. Sensitive intellectual property and privileged user credentials remain safe from theft.

Wi-Fi and Carrier Network Connections

FIPS 140-2 Compliant Connector with AES 256-bit Encryption

Your Organization's IT Infrastructure

BYOD with SentinelSecure™ Containerized App Workspace