

BYOD SPECIAL

# CIOReview

MAY 20 - 2015

CIOREVIEW.COM

Company of the Month



Danny Windham, CEO  
Digium

## SyncDog: The Enterprise Mobility Watchdog

Jonas Gyllensvaan,  
CEO & Founder

\$15 US



CIO REVIEW  
44790, S Grimmer Blvd.  
#202, Fremont, CA-94538

# *SyncDog:* The Enterprise Mobility Watchdog

By Aishwarya Kannan

**T**he corporate workforce is changing: Millions of employees who used to stay chained to their cubicles are now setting up the office wherever and whenever they find an internet connection. With an ever-widening range of devices—smartphones, tablets and laptops—these workers aren't limiting themselves to the company-provided hardware.

This trend—called BYOD—is creating a friction between what workers want and what companies need. To the workforce, a phone is personal, a place to work and play. But to the security team at the company, it's an open pit of danger. The reasons are manifold. A new Gartner report on BYOD and security states that 75 percent of mobile apps will fail security threats through end of 2015, leaving businesses vulnerable to attacks and violations of their security policies. “This risk is too high to ignore,” says Jonas Gyllensvaan, CEO and Founder, SyncDog.

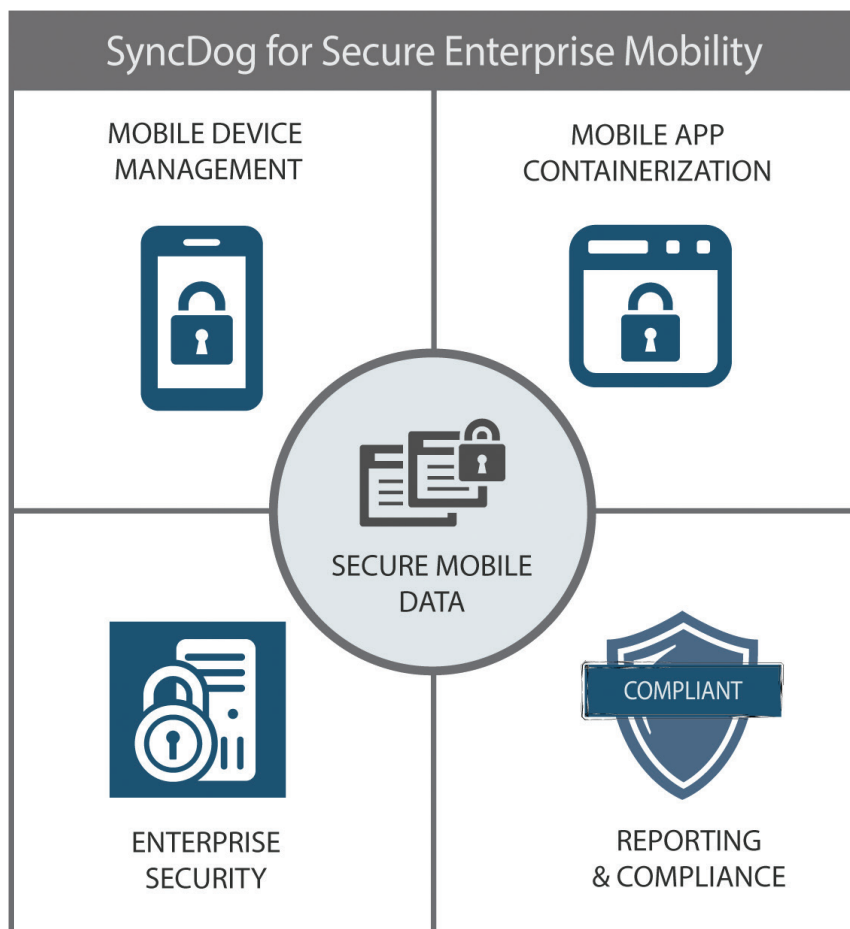
Enter SyncDog—a Vancouver-based company that is in the centre of harmonizing this enterprise BYOD and security correlation. With a powerful combination of low overhead and predictive intelligence, for all of today's mobile platforms, SyncDog seamlessly incorporates BYOD into the clients' workplace.

The success of a BYOD strategy depends on providing users the right interface which is not only secure for the corporation, but also highly collaborative and functional for day-to-day activities,” notes Gyllensvan. With pure software solutions that solve mobility service and security dilemma for enterprises, Gyllensvan believes that Enterprise Mobility Management (EMM) will be at the core

of protecting corporate data. “EMM has broadened in the past couple of years to include a number of different aspects,” says Gyllensvan. “The key is for companies to first understand their security tolerance and then implement the right type of solution. Understanding what is at risk, how it is at risk, and the potential fallout from a ‘data loss’ event should be the baseline for defining an EMM strategy,” he adds.

## A BYOD Culture

“Most of the network compromises that happen today are caused by careless users and malicious apps,” affirms Gyllensvaan. SyncDog takes a unique approach to help enterprises tackle this. The firm's flagship product, SyncDog Sentinel is built on the understanding that the real risk relates less to the device and more to the data which is stored and transacted through the device. The product provides a rich mobile end user experience with the ability to collaborate across a number of different software including Office Suite, PDF Annotation, Network File Share and Sync, and communication tools like Email, and Instant Messenger. It is designed to handle the complexities of diverse, large-scale enterprise IT environment and offers several flexible deployment scenarios. This gives Sentinel the power to negate security risks from stolen devices and accidental data leaks. It provides IT administrators with enterprise-level visibility that helps them focus on application delivery. The product's predictive intelligence feature helps administrators understand and uncover security vulnerabilities in their network, way before it becomes a big problem. SyncDog Sentinel These scenarios include basic implementation and Single Relay server Implementation and



Dual Relay Implementation, with load balancing by priority and also with SQL synchronization. Gyllensvaan also explains that data in applications can be protected by embedding the application within the SentinelSecure™ container where users can freely move from one application to another without ever leaving the secure container. This results in encryption of data at rest and in transit, while offering command and control over authentication, policy and application provisioning. Another area where SyncDog remains flexible is in the development of customized policies for the deployment of SentinelSecure. “Whether it is a contextual policy relating to the time of the day or a user’s geographic location, every organization needs flexibility in regulating corporate data,” says Gyllensvaan.

“**One of the benefits of our size is that we can quickly adjust to customer requests and make revisions to suit these requirements to meet the overall product strategy**”

The company also provides endpoint security and integrity—without a differentiation between the two. “We are primarily focused on improving the end-user experience while not compromising their security. This requires us to continually develop new and flexible policy options for secure container functionality to help companies deploy the required business applications without taking on high levels of risk,” states Gyllensvaan.

### Understanding Security Tolerance

SentinelSecure allows for app investments to be easily integrated into the EMM deployment, protecting the data in a secure environment. When it comes to EMM, being compliant with industry standards like Health Insurance Portability and Accountability Act (HIPAA), The Sarbanes-Oxley Act (SOX), and Federal Information Security Management Act (FISMA) also prove the integrity of the solution. Designing programs to custom-fit clients’ needs keeps the service cost-effective as they only have to pay for the features they use. Once deployed, the framework allows for unlimited additions which help businesses to easily mobilize their workflow.

Besides mobilization, Gyllensvaan feels that the creativity in the EMM marketplace has been stifled due to commoditized Master Data Management (MDM) services. The simple device control will soon migrate to complex policy management with new types of context like time,” says Gyllensvaan. SentinelSecure is ready to take this step, setting new standards in secured mobility.

### A Clear Defined Project Goal

SyncDog works closely with every client to fully understand the use cases in the BYOD spectrum to ensure clarity in definition of project goals. “The key to success in the BYOD landscape is to be surrounded by the right people who are not only smart and efficient, but who can also build close connections. It is

important to have a cohesive team who work together to find and understand initial customers with a laser focus on ensuring product development requirements,” says Gyllensvaan. The company’s flexible and scalable architecture enables the employees to completely prioritize market needs instead of being concerned about product limitations. “One of the benefits of our size is that we can quickly adjust to customer requests and make revisions to suit these requirements to meet the overall product strategy,” he affirms.

“


**Success comes from providing the user an interface which is quietly secure for the corporation, but highly collaborative and functional for day to day activities.**

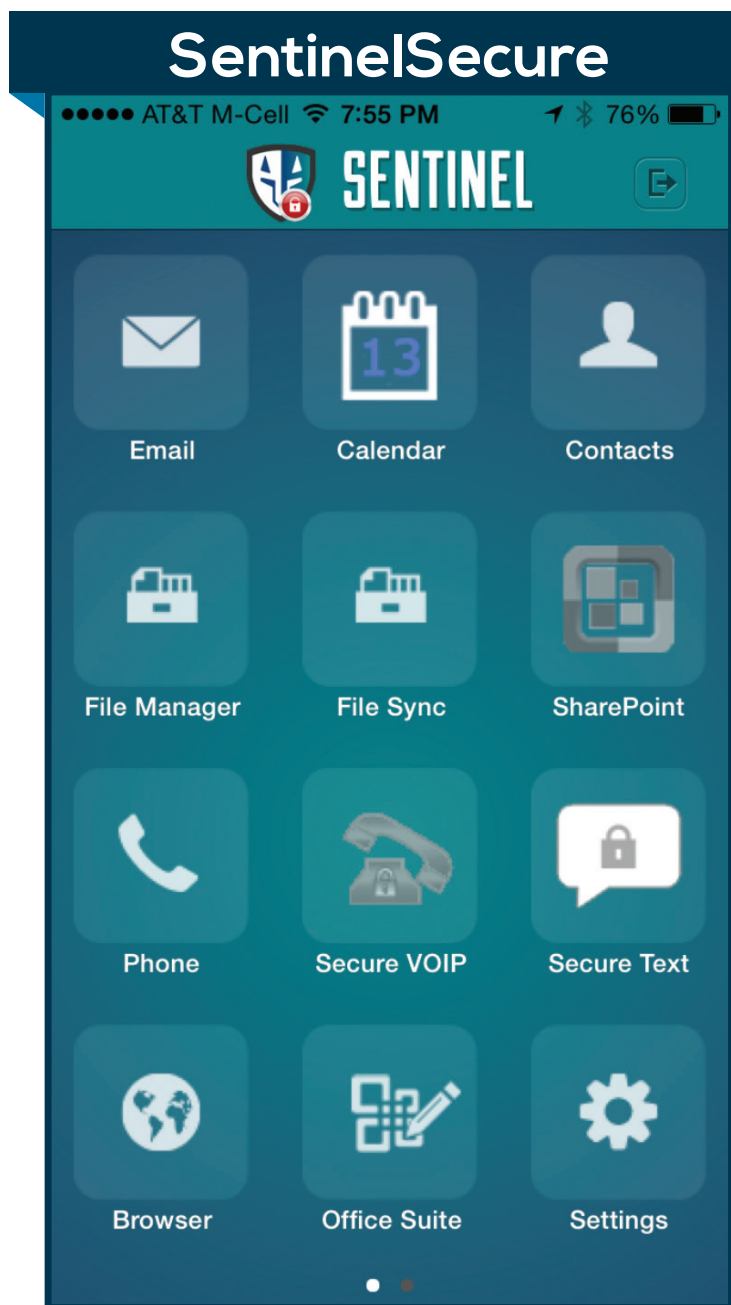
**Applications have become the new evolution in securing data**

### BYOD Productivity Spectrum

Moving ahead, SyncDog is bent on their key strategy of collaboration and partnerships. “We see ourselves as being one of the key providers for many vendors, and our goal is to make sure that vendors build value to their own brand,” says Gyllensvaan. SyncDog’s partners get access to more or less one stop shop security. Further, the company’s products are built around the ability to integrate and provide white labeling solutions. This makes it easier for any security vendor to enter the market with little or no infrastructure and security development costs.

Gyllensvaan illuminates that the security market has been exploiting consumers in the past. Proper security will still have a price tag attached to it and it will be a premium service. But the overall price point from security standpoint will decrease eventually. With regard to the end user policy, the company plans to regularly increase the number of business applications and infrastructure support available within SentinelSecure, which will provide context-capable deployment of end user policy. The company also plans to release new features like geo location and geo-fencing using GPS data and the functionality of time-sensitive policy enforcement in late 2015, which would be performed using GPS data from SyncDog’s partners including features like time-sensitive policy enforcement projects.

“We can never predict what the next big thing will be, but an open explanatory approach with current and potential customers yield a clear-defined development plan for the next few months. The roadmap of a company can change very quickly based on market events or changes, so being well aware of the marketplace and being open to change are key to finding success in this field,” concludes Gyllensvaan. 





## The SyncDog SentinelSecure Container: Enterprise Mobile Application Security and End-to-End Transactional Monitoring



### THE ULTIMATE OBJECTIVE:

Balance corporate data governance and end user productivity, while controlling costs and simplifying deployment.

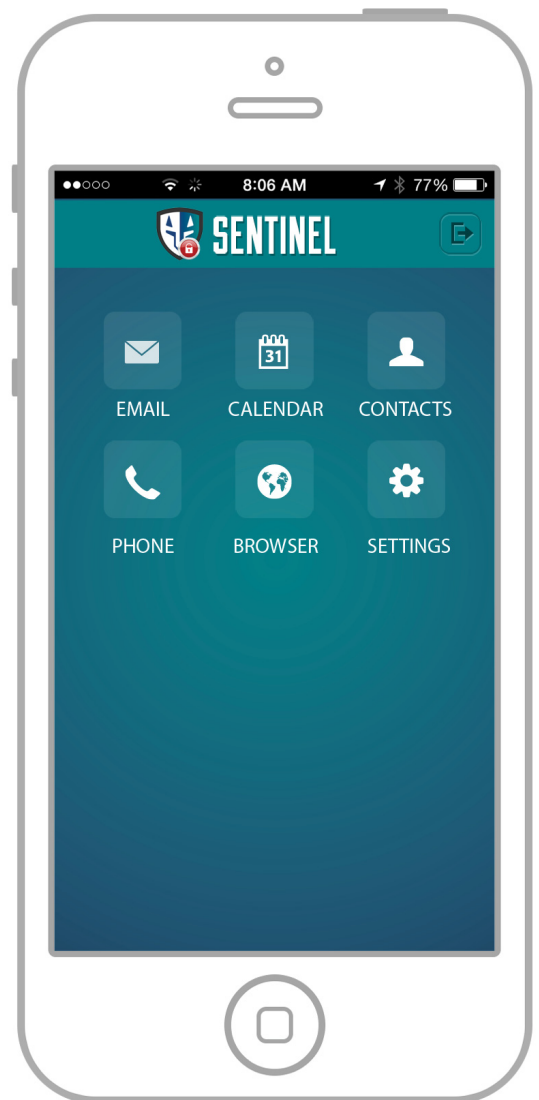
### THE ANSWER:

The SyncDog SentinelSecure Container allows your organization to control and manage how the people on your infrastructure exchange relevant, time-critical information across their wireless devices.

#### **Secure Corporate Data:**

#### **The SentinelSecure Container**

- To reduce the potential for network breach, corporate and personal applications are segmented via container
- Defense-Grade Secure Workspace for Corporate Data Security & Compliance
- Prevents both data leakage and virus/Trojan/malware intrusions
  - » User may copy and paste within container, however, users cannot copy and paste in or out of the container
- Provides military-grade encryption for data at rest and in-transit (FIPS 140-2 AES 256)
- An email solution that includes both S/MIME and CAC capabilities
  - » Full-featured clients for Microsoft Exchange with support for HTML e-mail, attachments, calendaring and contacts
- Secure Browser with CAC capabilities
  - » Ensures users have a seamless experience whether browsing the corporate intranet or the public Internet.
- Secure instant messaging
  - » Integrates with MS Lync, MS Office Communicator, and Google Talk



- SentinelSecure SDK allows for third-party integration for iOS and Android devices
  - » Prevents reverse engineering and allows for Data Protection, App Compliance, App-Level Threat Defense, Security Policy Enforcement, and App Integrity
- Secure Camera
  - » Pictures taken stay in the container



## The SentinelSecure Server

- End-to-end transactional monitoring for smartphones and infrastructure devices.
- IT-managed access controls, usage policies and remote commands.
- Ensures organizations can prove compliance in an auditable fashion.
  - » SentinelSecure uses a standard relational database management system for storing and managing data about each mobile device – user data, software, and system-level configuration information
- Secure connectors for browsers, applications and ActiveSync.
  - » Prevents the need to expose existing corporate infrastructure components to the internet.
- Adheres to corporate current corporate web browsing management restrictions
  - » Routes traffic through the corporate proxy/firewall and authenticates the user ensuring appropriate browsing rights and restrictions are granted
- FIPS 140-2 AES 256-bit data encryption
- Hardware-separated Multi-factor Authentication (MFA)
- Resilient no-NOC architecture.
  - » **Cost effective:** Does away with charges for NOCs, allows for negotiation of contracts with wireless data rates that do not include hidden NOC charges. No longer a need for a private leased line, or a private frame relay or (IP/MPLS) connection, to connect to the NOC independent of the supplier of wireless e-mail technology.



- » **More secure:** Prevents temporary external storage of a user's email on the NOC and out of the organization's control, when the user is out of coverage. Avoids any concern about NOC's security being breached, and undetected hostile traffic entering the NOC and through to your corporate gateway or email gateway.
- » **Limit service disruptions:** To deliver a good service, all connections between the gateway, the NOC and the mobile network must be working at all times. The NOC is outside of the company's control. Eliminating one additional component (the NOC) reduces the risk of a major service disruption.
- Support for S/MIME and CAC (Common Access Cards)
  - » SentinelSecure Container meets the Defense authentication agencies requirement – CAC
  - » SentinelSecure Container meets financial institutions requirements to encrypt confidential client information - S/MIME
- Relay Server is the only appliance that requires exposure to the Internet and can support different setups
  - » Can be placed outside the corporate firewall
  - » Can be placed in the DMZ
  - » Can be behind the firewall with only the communications port open

### ***Improve Productivity:***

*Allow business users to easily and quickly access the data they need.*

### **The SentinelSecure Container**

- Full-featured clients for Microsoft Exchange with support for HTML e-mail, attachments, contacts and OTA calendaring
- Smart Office gives the ability to easily view, create, edit, print and share documents
- PDF Annotate allows users to view, add notes, and comments to an existing document.
- Access corporate approved applications
- Access to file shares to view, retrieve or save documents



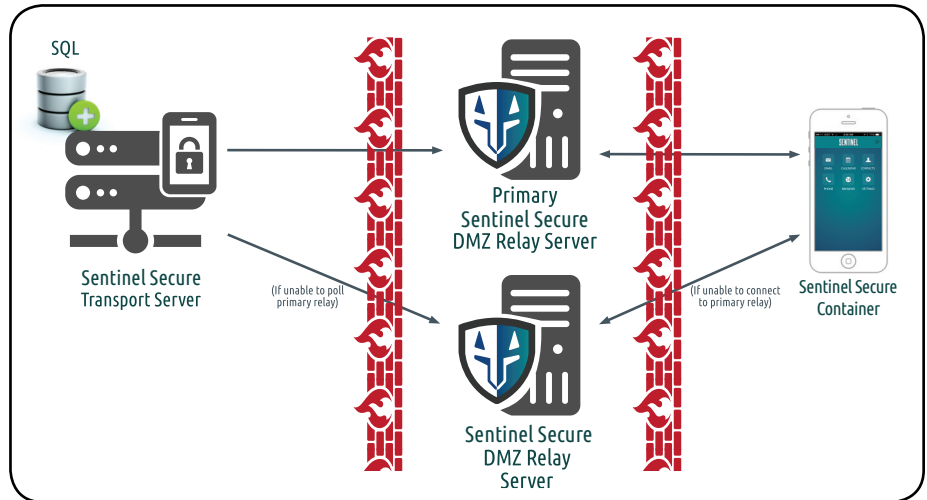
## ***Ease of deployment:***

### **The SentinelSecure Server**

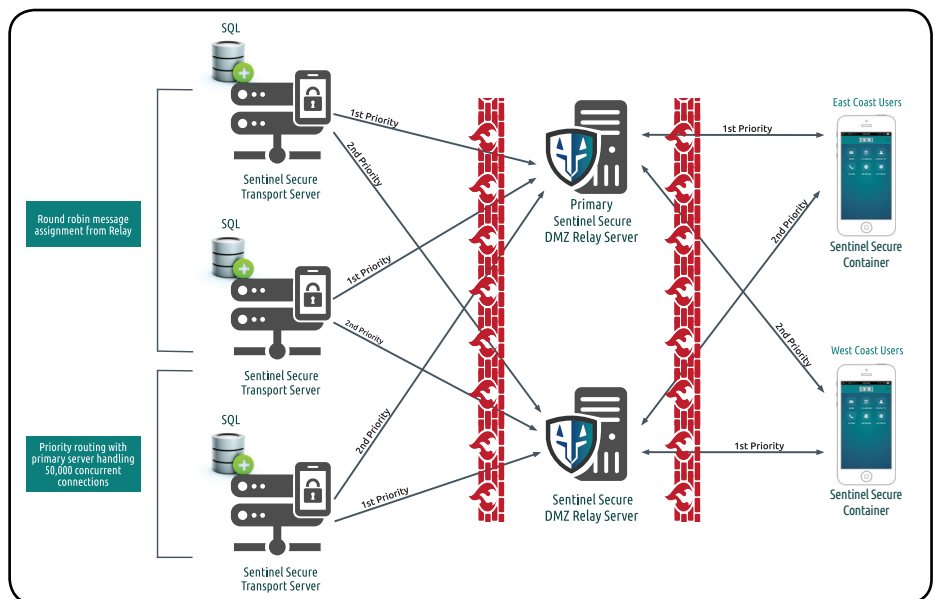
- Support popular smartphones and tablets whether BYOD or Corporate Owned
- Flexible deployment options – single- or multi-relay server with transport load balancing and failover. This approach gives it the ability to handle the volume of connections from diverse mobile operating systems in large enterprise environments, without compromising system performance and availability.
- Complementary solution that leverages your existing technology to protect previous IT investments
- Single enterprise system - complete, integrated system with single UI, no need to learn different UIs for different pieces of functionality
- Centralized administration of device provisioning, configuration and security
- Remote mobile client administration from central location with query, over-the-air lock or wipe

### **In Summary:**

Ultimately, the SyncDog SentinelSecure Container delivers secure mobile enterprise collaboration with end-to-end transactional monitoring, and provides an audit trail for maintaining compliance standards.



*SentinelSecure Dual Relay Implementation*



*SentinelSecure Load Balancing by Priority Implementation*