SYNCDOG

Product Overview

SyncDog Enterprise Mobility Solution

- *Mobile Security Event Management*
- *Mobile Device Management*
- *Mobile Application Security*
- *Compliance & Reporting*

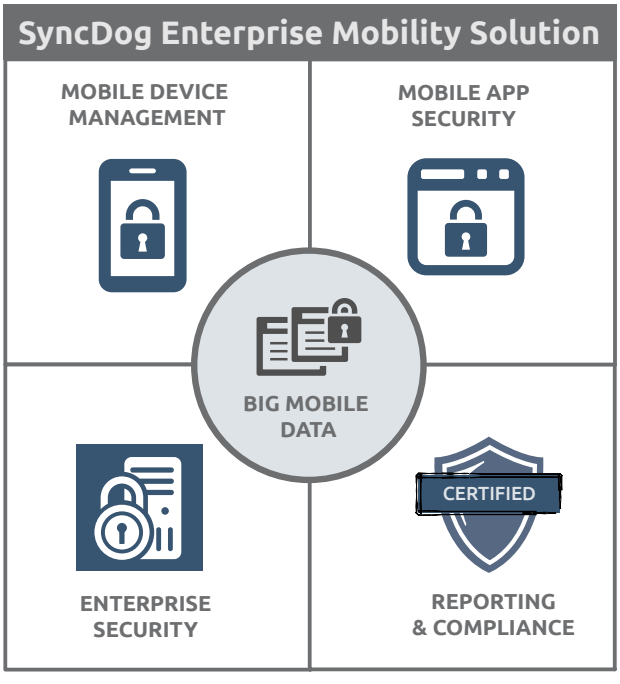
Bring-your-own-device (BYOD) and the need to harmonize personal and corporate computing into a secure and compliant environment are creating a seismic shift in enterprise IT today. We can now safely conclude that most business professionals will use a smartphone and/or tablet to access and store both personal and business information on the same device. In concert with this, many organizations are now supporting both company-liable and employee-owned mobile devices as a way of boosting productivity and reducing costs.

In this new world of enterprise mobility, the benefits to both the organization and the employee can be significant. However, the task is becoming increasingly difficult as a host of new threats and vulnerabilities are exposing mobile devices to greater risks like corporate data leakage, privacy loss, cyber-attacks and regulatory compliance breaches. Being sued, fined or shut down as a result of data being compromised, misused or lost is becoming a greater risk every day for organizations in regulated industries.

This surge in mobile connectivity is expanding network complexity like no other technology has done since the Internet explosion of the 1990s. Unfortunately, the by-product of this expansion is an increase in the attack surface of your IT network, leaving your intellectual property and compliance to risk like never before.

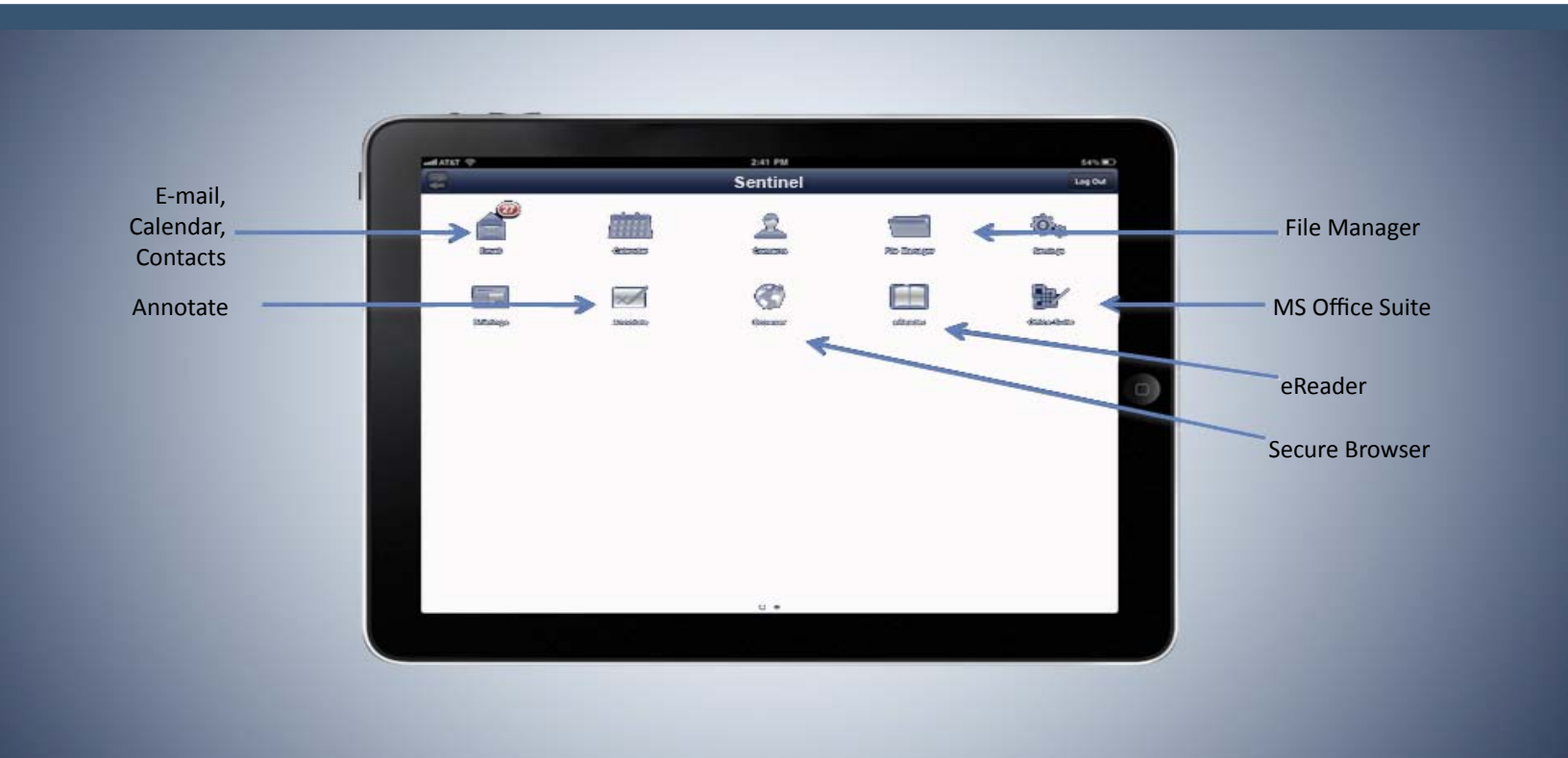
SyncDog's Enterprise Mobility Solution can help secure and manage your network, verify system integrity, and maintain compliance without negating the benefits of a mobile workforce. SyncDog EMS leverages Big Mobile Data and uses that data to:

1. *Manage the provisioning of mobile devices*
2. *Manage application security, deployment and containerization*
3. *Manage device/network security*
4. *Maintain compliance and reporting standards*



The SyncDog EMS product portfolio consists of:

- **SyncDog Sentinel** for centralized mobile device management (MDM), including provisioning of mobile devices and management of IT policies, users, applications and mobility infrastructure. Sentinel is the cornerstone of SyncDog EMS and does the bulk of end-to-end monitoring and data collection for device performance, availability and security. Sentinel also handles personal identity management through hardware separated multi-factor authentication.
  - » SyncDog Sentinel includes server-side software components which act as the main point of management, administration and reporting for IT. These server components use a standard relational database management system for storing and managing data about each mobile device, user and the software residing on them, as well as system-level configuration information. The server components include the necessary services for issuing remote IT policy commands to mobile devices and to retrieve custom reports and data from each mobile device on the network.
  - » SyncDog Sentinel also includes "agent" software that runs locally on mobile devices and mobility infrastructure components, such as BlackBerry Enterprise Server and Good Technology servers, to enable local scanning of software configurations and system log files.
- **SyncDog Sentinel Secure** allows an organization to control and manage how their people exchange relevant, time-critical information across their wireless handheld devices. Sentinel Secure allows your IT to establish and enforce secure enterprise-wide policies to protect everyday collaboration and communication. Sentinel Secure leverages AES 256-bit encryption to keep business data and apps in containers that are completely under the control of the organization's IT, without impacting the personal side of the device.
  - » There are three different versions of Sentinel Secure's containerized solution:
    - Client-side only version that users can easily install on their devices
    - Client/server version administered by a systems admin
    - Client/server version with and SDK/API
  - » With complete centralized control of mobile computing across the enterprise, the organization has the ability to deploy multiple geographically disparate relays throughout the NOC thereby avoiding a single point of failure. Deploying multiple relays in multiple locations throughout an enterprise provides multiple failover options. The Sentinel Secure handheld device software provides the intelligence to allow the device to connect to any relay in the enterprise without user interaction.



  - » Sentinel Secure is more reliable than other wireless messaging systems because it does not rely on a centralized network operations center (NOC). The Sentinel Secure relay resides inside the organization's network, giving administrators complete control of the relay(s) and the data that resides on them. All messages and data remain safely within the organization's security perimeter until destination devices are ready to receive and process the data. With Sentinel Secure, any installation can be configured for hot failover to an alternate computing facility or geographically dispersed and redundant relays.
  - » Sentinel Secure uses a Smart Certificate that an admin can wirelessly set and change configuration parameters such as the primary or secondary Sentinel Secure Relay for a user. A power outage or disaster affecting one relay will not interrupt a user's ability to access the network since Sentinel Secure will automatically check for authenticated back-up relays in the network and installed in the Smart Certificate. Sentinel Secure can act as the backbone for a secure broadband wireless data exchange between "behind-the firewall" enterprise applications and handheld devices.
  - » SyncDog's Sentinel Secure solution is a software-based, secure data platform. The system uses FIPS 140-2 certified AES 256 bit encryption for both data at rest and data in transit between an enterprise-based server solution and a secure, partitioned application on a user's device, including iPhones, iPads, Android Smartphones, or other handheld PCs.
  - » Sentinel Secure allows users to enjoy all of the dynamic features of their device, while maintaining a separate and encrypted portion of the phone for all enterprise business-related information.
- **SyncDog Event Log Manager** ensures intellectual property is secured through a device log management system that collects user events and correlates them for anomalies that could be indicative of threat. When a potential threat is exposed, the system can automatically generate a help-desk ticket for actions with priorities.
  - » SyncDog Event Log Manager can handle a steady stream of 2,000 event message logs per second, with the ability to handle burst speeds up to 10,000 per second. Each log is indexed for quick search and the solution has data normalization capability that formats unstructured data for use in a relational database.
- **SyncDog EMS for Reporting and Compliance** – SyncDog EMS provides a host of bundled reports for compliance and cyber-threat detection right out of the box. These reports can be easily customized to fit business requirements and the system can be set up to send reports to any e-mail address at any scheduled interval. All SyncDog out-of-box reports adhere to the stringent requirements set forth by PCI DSS, HIPAA, Sarbanes-Oxley, and many other industry standards.

SYNCDOG

PRODUCT FEATURES: SyncDog Sentinel Device Manager

- Cross platform mobile device management
- BlackBerry Enterprise/Good Technologies server monitoring
  - » Real-time log management provides up-to-second device performance/availability metrics
- Real-time compromise detection utilizing a device agent providing continuous scanning
  - » Help-desk integration for fast alerts and quick remediation
- AD/LDAP integrated
- Role-based administration with activity auditing
- Centralized administration - A web-based administrator interface provides full control over your Sentinel deployment. Search for devices, perform instant over-the-air lock or wipe. Set customized security messages.
- Centralized event log management and system log storage/archiving for forensics and compliance
- Mobile client administration - Provides administrative access from anywhere, including remote lock/unlock and wipe capabilities.
  - » Transparency - End-user sees nothing unless device is compromised and locked or wiped
  - » Real time agent-based device scanning
  - » Real-time status updates send to administration console for compliance reporting
  - » Tamper proof - Sophisticated application peer monitoring system ensures client cannot be removed or compromised
  - » Query, remote lock, remote unlock, or wipe from remote admin console

PRODUCT FEATURES: SyncDog Sentinel Secure

- Device containerization with encrypted corporate workspace with IT-managed access controls, usage policies and remote commands
  - » E-mail with S/MIME and CAC
  - » Calendar and Contacts
  - » Office and PDF Document Suite with view, create, edit, annotate
  - » File Manager

SYNCDOG

  - » Secure Browser and Camera
  - » Application wrapper SDK
- Supports Android, iOS, and BlackBerry
- Defense-Grade Secure Workspace for Corporate Data Security & Compliance
  - » FIPS 140-2 AES 256-bit data encryption
  - » Hardware-separated Multi-factor Authentication (MFA)
  - » Resilient no-NOC architecture
  - » Support for S/MIME
  - » Proxy server behind-the-firewall
  - » Secure connector for ActiveSync
  - » Secure connector for browser and apps
- Ensures organizations can prove compliance in an auditable fashion.
- Supports integration with existing enterprise mobility infrastructure including BlackBerry Enterprise Server and Good™ Technology server deployments
- Full-featured clients for Microsoft Exchange with support for HTML e-mail, attachments and OTA calendaring

PRODUCT FEATURES: SyncDog Event Log Manager

- High Speed Message Reception – capable of processing more than 2,000 messages per second and can handle burst traffic of more than 10,000 messages in one second.
- High-speed message correlation and filtering – uses an advanced correlation engine, which performs semantic analysis of event log messages in real-time.
- System employs correlation threads, correlation counters, correlation alerts, and correlation triggers, which refine and reduce incoming messages into actionable intelligence.
- Data Searching Ability – uses proprietary GenDex technology, which employs a high speed, real time index system allowing quick searches through massive amounts of message data
- Capable of searching one terabyte of data for a particular keyword in less than one second.
- Correlation engine linked to help-desk automation systems for immediate and prioritized actions
- Data normalization technology allows users to define own categories by removing “facility” code restrictions. This allows data to be highly structured for relational databases.

BYOD *Facts*

1. 76% of IT execs surveyed say that they are permitting employees to use their personal laptops, tablets and smartphones.

2. Security breaches have been experienced by 46.5% of all companies that allow BYOD.

3. 80% of companies surveyed have an acceptable use policy (AUP) but only 12% have remote device wipe provision when a device is lost or stolen.

- TrendMicro report on mobile consumerization

SYNCDOG

PRODUCT FEATURES: Compliance and Reporting

- 100s of reports for auditing, performance, usage patterns and more
- Hundreds of metrics defined
- Real-time or long term trending
- Deep-use behavior analytics to understand application use by device
- Centralized logs on a single system - aggregates log files from diverse systems into a single repository, backing up all device data into a single tamper-proof location.
- Provides the empirical proof to verify compliance with a single audit trail. SyncDog provides detailed, automated reporting to compliment audits, dramatically reducing resources required to prepare audits.
- Out of box reports include:
  - » Privileged user activity, including accounts modified/created activity
  - » All user activity
  - » All perimeter activity
  - » All account activity
  - » Most active users
  - » Locked-out accounts
  - » Intrusion detection
  - » Firewall warning

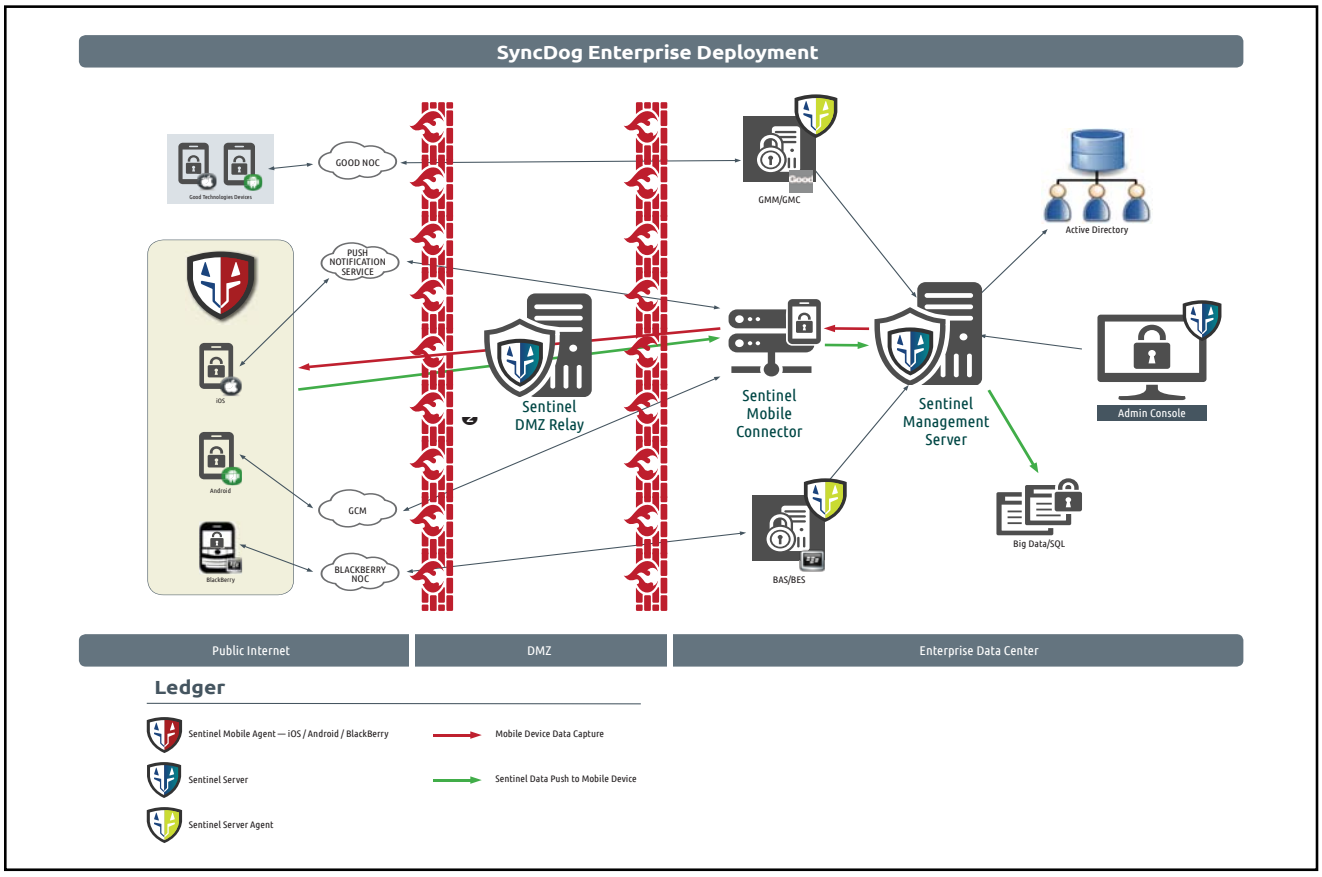
BENEFITS

- Maintain and prove compliance with internal policies and government regulations
- Low Total Cost of Ownership – reduce costs by 40-50%
- Prevent security breaches, cyber attacks and policy violations
- Protect and encrypt private corporate data on iPad, iPhone, Android and BlackBerry devices
- Systematic and compliant way to manage BYOD
- Centralize management of all mobile devices
- Maximize productivity by enabling corporate e-mail, browsing and apps without compromise
- React quickly to mobile device and BYOD trends while ensuring you can manage your risks and report on compliance

- Highly scalable distributed architecture
- Real-time analytics and reporting facilitates many industry standards such as PCI DSS, HIPAA, Sarbanes-Oxley, and other requirements.

SYSTEM ARCHITECTURE

SyncDog's Enterprise Mobility Solution is deployed as a behind-the-firewall solution with the following system architecture:

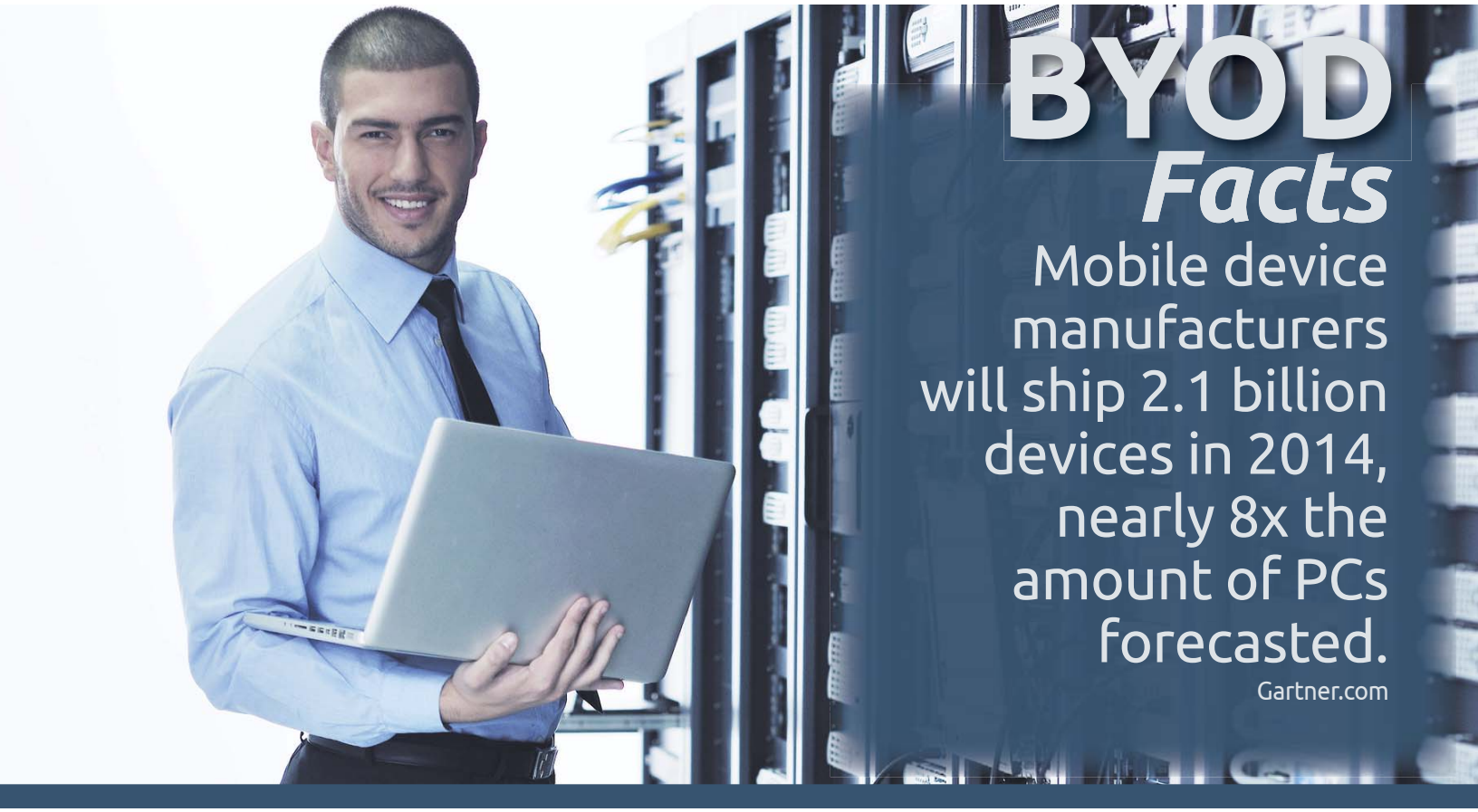


System Components

SyncDog Sentinel Management Server — Provides the core functionality for SyncDog Sentinel MDM. The SyncDog Sentinel Management Server is the primary server for managing devices, and provides much of the administration and reporting functionality via a web-based management console including device and user management, security and policy management, remote lock/wipe commands, and comprehensive reporting across your mobility deployment. This server also provides optional monitoring of BlackBerry Enterprise Server and Good Technology infrastructure.

SyncDog Sentinel Mobile Connector and DMZ Relay — The SyncDog Sentinel DMZ Relay must reside in the DMZ and will act as a proxy for the information received by iOS and Android devices. This information is sent to the SyncDog Sentinel Mobile Connector, a server that must reside within the corporate network. This server is also able to initiate device transactions by communicating with the Apple Push Notification Service (APNS).

SyncDog Sentinel Mobile Agents — The SyncDog Sentinel Mobile Agents run locally on smartphones and tablets. The agent for Android is responsible for performing device integrity scans, monitoring and reporting for SyncDog Sentinel Integrity Services, and for managing local execution of SyncDog Sentinel MDM commands. The agents for BlackBerry and iOS are responsible for performing device integrity scans and monitoring and reporting for SyncDog Sentinel Integrity



The BlackBerry Server Agent resides on a BlackBerry Enterprise Server and is responsible for on-server monitoring and reporting. The Good Server Agent resides on a Good Technology GMC server and is responsible for proxying administration commands from the SyncDog Sentinel Management Server and monitoring the GMC and GMM server log files. The SyncDog Sentinel Server Agents are optional components, and are only required for customers who wish to use SyncDog Sentinel to centrally monitor their BlackBerry or Good Technology server deployments.

Mobility Infrastructure Management

In addition to managing mobile devices and users, SyncDog EMS can be used to centrally monitor and manage the following mobility infrastructure servers:

BlackBerry Enterprise Server — Automated monitoring of BlackBerry Enterprise Server log files to identify and report on infrastructure, service and performance issues. The system detects changes in server and infrastructure operating patterns and applies predictive analysis techniques to detect declining service levels that may lead to outages or BlackBerry service disruptions. Additionally, SyncDog EMS provides detailed reporting and analytics to track data usage patterns, service interruptions, and other information that can be used to enhance monitoring and management of BlackBerry infrastructure and device users.

Good Technology Servers — Automated monitoring of Good Technology server log files and error reporting to identify and report on infrastructure, service and performance issues. Detects changes in server and infrastructure operating patterns and applies predictive analysis techniques to detect declining service levels that may lead to outages or Good Technology service disruptions.

CONCLUSIONS AND SUMMARY

SyncDog EMS is a powerful and flexible mobile security and risk management solution that enables IT organizations to centrally manage mobile devices and enterprise mobility infrastructure, monitor and detect tampering and OS vulnerabilities, maintain policy compliance, and ensure they can prove compliance in an auditable fashion. SyncDog EMS is the trusted solution for securing mobile devices and maintaining compliance across both the public and private sector.

With SyncDog EMS, IT organizations can centrally configure, manage, monitor and report on their growing deployments of mobile devices and mobility infrastructure. With centralized management of mobile users, devices, applications and IT policies, as well as integrated monitoring of enterprise mobility infrastructure, SyncDog Sentinel MDM gives IT organizations a "single pane of glass" for securing and managing their entire mobility deployment.

And because SyncDog EMS provides comprehensive support across BlackBerry, iOS and Android devices as well as the related IT infrastructure, it provides a complete framework to help IT organizations transition from a controlled homogeneous mobility environment to a more open and flexible heterogeneous environment supporting multiple platforms and devices without compromising on security, manageability, governance or compliance.

To learn more about SyncDog EMS and our growing portfolio of defense-grade mobile security and risk management solutions, please visit us at www.SyncDog.com or contact us at sales@SyncDog.com to request a trial today.

SYNCDOG

SyncDog, Inc.
1818 Library Street, Suite 500
Reston, VA USA 20190
Call: (703) 430-6040 | Fax: (703) 997-8667
sales@syncdog.com • www.syncdog.com

About SyncDog

To overcome BYOD challenges, IT administrators need real-time visibility into the service status of every device on the network, regardless of ownership.

Mobile professionals are the new norm and downtime is a productivity killer.

Mobile Enterprise Security Correlation made simple!