SYNCDOG

Case Study

SENTINELSECURE INFRASTRUCTURE AND SENTINELSECURE CONTAINER:

Industry: Law Enforcement

Client: Large Metropolitan Police Department

Customer Objectives

A critical component of solving a crime is the reconstruction of the crime after gathering information from the crime scene. Crime scene reconstructing cannot take place without proper evidence gathering. This case study documents the use of SyncDog SentinelSecure™ to gather photographic and video crime-scene information on tablets, phones and cameras with Android OS's installed in a U.S.-based municipal police department (MPD).

Why SyncDog?

A recent security audit by the MPD revealed three things about the processing of crime-scene data:

1. The workflow for getting crime-scene data to their secure datacenter created elevated risk levels for data loss.
2. Images, video, voice recordings and SMS texts were not secure and segmented from personal data on employee devices.
3. It was taking too long to get crime-scene data into MPD's secure network environment.

Crime scene processing is often chaotic and unpredictable. Upon arrival, the first law enforcement responder must determine the size of the crime scene before any evidence is gathered. Adherence to workflow and process for the initial assessment of the scene and subsequent information gathering are critical success factors in solving and preventing future criminal activity.

The MPD audit determined that the process of uploading data to the secure datacenter was cumbersome and risky. When a tech or detective took a series of images, video, or voice recordings from the crime scene, the process was to remove the SD card from the device, load it into a laptop SD slot, copy to the hard drive, then upload to MPD's secure network environment. On at least one occasion, either the SD card or the laptop was lost or compromised, putting the success of the investigation at high risk – i.e. information was leaked to the public. Additional to the security risk was the time it took to get the crime-scene data to MPD's secure network store. In some instances, the lag time was hours later, after the tech or detective returned to the office or suitable location to transfer the SD images/videos/recordings to laptop then to MPD's secure datacenter.

Auditors also found that on personal devices, SMS texts about the investigation were found. There was no policy for segmenting communications about investigations off of personal devices; meaning, all personnel could send/receive texts about the investigation, regardless of if the devices were BYOD or COPE (corporate owned personally enabled). This was another instance of crime-scene information at high risk of being released to the public.

SENTINELSECURE INFRASTRUCTURE AND SENTINELSECURE CONTAINER

FAST DEPLOYMENT.

EASY TO CONFIGURE.

INTUITIVE TO LEARN.

The SyncDog Sentinel Infrastructure Framework and SentinelSecure Container™ were installed in a multi-phased approach. First, the Sentinel Framework was installed on a VM (see Figure 1, at right).

Next a small group of users was added to the framework with SentinelSecure™ container installed on various mobile devices. The installation took less than two days. Users log into SyncDog on their devices and work as normal in a UI very similar to the operating system on the device (see Figure 2, below).

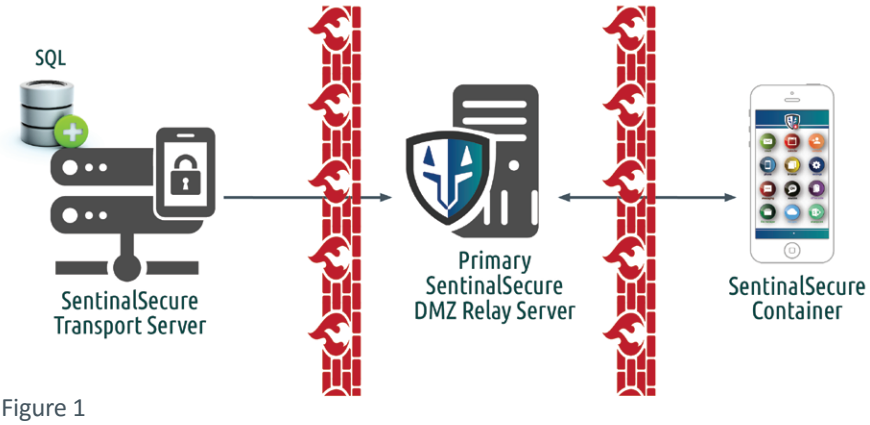

Figure 1
SentinelSecure simple infrastructure architecture with single relay transport server

Results from deploying the SyncDog Framework and Container

With SyncDog Sentinel Infrastructure Framework and SentinelSecure Container™, the workflow and compliance for handling of crime-scene data have shown dramatic improvements.

- The workflow for getting images, video and audio recordings to the secure network data store has been dramatically streamlined. Essentially, today when an image or video is captured, automation sends the data immediately to the secure network. The need to transfer with SD card via laptop has been eliminated, the risk to lost data reduced.
- With the addition of the SyncDog SentinelSecure™ container, law enforcement images, video, texts, and other recordings are segmented from personal data and high-risk personal games/applications. The container "wraps" the law enforcement data in a secure environment protected by FIPS 140-2 grade encryption with an AES 256 algorithm.
- With the simplification of the crime-scene processing workflow and added security, detectives and crime-scene techs can focus more on police work and worry less about auditing and compliance while investigating.

Figure 2

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