SYNCDOG

Use Case Study: High Risk Regions

Ensuring Secure Mobile Communications for a Security Services Organization in High-Risk Regions Overview

A Security Services Organization operating in a highly sensitive region faced significant challenges in securing mobile communications for its freelance operatives. These operatives, who are not direct employees, rely on personal mobile devices to report on critical issues in war-torn and heavily militarized areas. Given the heightened risk of government surveillance, hacking, and device confiscation, the organization needed a robust security solution that would ensure operational security, protect the identities of its operatives, and safeguard sensitive data.

Challenges

1. **Vulnerability of Mobile Devices**: Mobile devices are increasingly targeted by cyber threats, surveillance programs, and unauthorized access attempts.
2. **Freelance Operative Model**: Operatives use their own personal devices (BYOD), making traditional MDM/EMM/UEM solutions unfeasible.
3. **Data Security and Privacy**: Full encryption of stored data (Data at Rest) and transmitted information (Data in Transit) was necessary to prevent government or military interception.
4. **Geo-Location and Safety Monitoring**: The organization required a way to track operatives' locations for safety without exposing them to undue risks.
5. **Remote Data Wipe Capability**: In case of device confiscation, loss, or an operative being detained, sensitive data needed to be erased immediately.
6. **Zero Trust Security Architecture**: The solution needed to mitigate threats such as man-in-the-middle attacks, SSL stripping, and unauthorized access.

Solution: SyncDog's Trusted Mobile Workspace

SyncDog's Trusted Mobile Workspace stood out by addressing the unique requirements:
The Security Services Organization selected SyncDog's Trusted Mobile Workspace due to its industry-leading security capabilities and ease of deployment on BYOD devices. Key advantages included:

1. **Military-Grade Encryption**:
   FIPS 140-2 certified AES 256-bit encryption for securing all sensitive email, files, apps, and data.
   Encryption applied both to Data at Rest (stored on the device) and Data in Transit (transmitted between operatives and the organization).
2. **Seamless Deployment on BYOD Devices:**
   No MDM agent required, ensuring operatives could easily install the solution without IT team intervention.
   Operatives retained control over personal applications and data, maintaining their privacy and autonomy.
3. **Geo-Location Monitoring & Safety Alerts**:
   Real-time location tracking helped the organization monitor operatives' locations to ensure they were safe.
   Alerts triggered when operatives moved out of expected locations or were forcibly detained.

1\.
2. Continued.....

4. **Remote Data Wipe & Threat Mitigation**:
   SyncDog's "time bomb" feature allowed for remote wiping of sensitive data in case of device loss, confiscation, or security threats.
   Root and Jailbreak detection prevented unauthorized access and exploitation of stored information.
5. **Zero Trust Architecture**:
   Protection against man-in-the-middle attacks and SSL stripping.
   Ensured all communication remained private, preventing government or military surveillance from intercepting sensitive information.
6. **Flexible Data Access & Secure Sharing**:
   Enabled rapid deployment of new operatives without requiring full device control.
   Allowed the organization to revoke access to sensitive data instantly once an operative was no longer affiliated with the organization—without affecting personal files, emails, or apps.

Result

By implementing SyncDog's Trusted Mobile Workspace, the Security Services Organization successfully:

- Ensured the integrity and confidentiality of sensitive data shared with freelance operatives.
- Protected operatives from government surveillance and unauthorized access while allowing them to work freely without fear of exposure.
- Provided a secure and flexible working environment without impeding the operatives' personal device use or privacy.
- Improved operational efficiency by allowing quick onboarding and secure communication with new operatives as needed.

Conclusion

The Security Services Organization chose SyncDog for its unparalleled ability to secure mobile data while respecting the autonomy and privacy of freelance operatives. With robust encryption, Zero Trust security, remote wipe capabilities, and geo-tracking for safety, SyncDog's Trusted Mobile Workspace delivered a best-in-class solution that successfully mitigated the risks associated with operating in highly scrutinized and dangerous environments

About SyncDog

SyncDog is a leading provider of endpoint security solutions, specializing in securing corporate data on mobile devices without compromising user privacy. Its innovative approach ensures data encryption and isolation, making it ideal for organizations with stringent security and compliance requirements. Learn more at www.syncdog.com.